

BBC

FOCUS MAGAZINE *Collection*

VOL.10

THE SCIENCE OF TRUE CRIME

The CIA on how
to spot a lie

Anatomy of
a crime scene

My life working
with serial killers

The psychopath
that sits next to you

The Boston Strangler

How a brain tumour can
turn someone into a criminal

The Golden
State Killer

How to beat
the hackers

The robocops
fighting crime

The Vampire
of Sacramento

Dead body farm

AI to predict
terrorist attacks



UCL

CERTIFICATE OF HIGHER EDUCATION IN ASTRONOMY BY EVENING STUDY AT UCL

Undergraduate Certificate in
two years of part-time study
beyond the level of ordinary
evening classes

No subject-related A-level
requirements

UCL's Physics and Astronomy
Department is top-rated for
teaching and research

One evening per week
at UCL from 6pm to 9pm,
near Euston Station

Regular practical classes at our
superbly equipped Observatory
at Mill Hill (below)

For keen amateur
astronomers, teachers, and
anyone interested in learning
more about astronomy



For more details see our website www.ucl.ac.uk/phys/admissions/certificate
Prospective students may also contact the admissions secretary by email
at astrocert@ucl.ac.uk or by phone on 020 3549 5807

EDITORIAL

Editor Daniel Bennett
Managing editor Alice Lipscombe-Southwell
Production editor Jheni Osman
Commissioning editor Jason Goodyer
Staff writer James Lloyd
Editorial assistant Helen Glenny
Additional editing Rob Banino

ART & PICTURES

Art editor Joe Eden
Deputy art editor Steve Boswell
Designer Jenny Price
Additional design Dean Purnell
Picture editor James Cutmore

PRESS AND PUBLIC RELATIONS

Press officer Carolyn Wray
carolyn.wray@immediate.co.uk

PRODUCTION

Production director Sarah Powell
Senior production co-ordinator
Derrick Andrews
Reprographics Tony Hunt, Chris Sutch

PUBLISHING

Commercial director Jemima Dixon
Content director Dave Musgrove
Publishing director Andy Healy
Managing director Andy Marshall

BBC STUDIOS, UK PUBLISHING

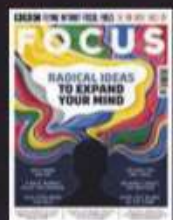
Director of editorial governance Nicholas Brett
Director of consumer products and publishing
Andrew Moultrie
Head of publishing Mandy Thwaites
UK Publishing coordinator Eva Abramik
Contact UK.Publishing@bbc.com
bbcworldwide.com/uk--anz/ukpublishing.aspx

CIRCULATION / ADVERTISING

Circulation manager Rob Brock

© Immediate Media Co Bristol Ltd 2018. All rights reserved. No part of *The Science of True Crime* may be reproduced in any form or by any means either wholly or in part, without prior written permission of the publisher. Not to be resold, lent, hired out or otherwise disposed of by way of trade at more than the recommended retail price or in mutilated condition. Printed in the UK by William Gibbons Ltd. The publisher, editor and authors accept no responsibility in respect of any products, goods or services which may be advertised or referred to in this issue or for any errors, omissions, mis-statements or mistakes in any such advertisements or references.

While every attempt has been made to ensure that the content of *The Science of True Crime* was as accurate as possible at time of press, we acknowledge that some information contained herein may have since become out of date. Also, the content of certain sections is occasionally subject to interpretation; in these cases, we have favoured the most respected source.



Like what you've read?

Then take out a subscription to *BBC Focus* magazine, the UK's best-selling science and tech monthly. Go to www.sciencefocus.com/subscribe for details.

**IMMEDIATE
MEDIA^{CO}**

Guilty pleasures



Most of us have a morbid fascination with crime. We may not like ourselves for it, but we can't help clicking on a news story about a serial killer or watching just a bit of a gory documentary as we flick through the channels. Why? What's the allure?

It's the spectacle – just like we 'rubber neck' a traffic accident on the motorway, a serial killer's actions may horrify us but we struggle to look away, because we get a hit of adrenaline. Plus, we love to be scared – provided it's in a protected environment. From the safety of your sofa you can get the heart pumping watching some horrific crime drama. And a series lets you join in the fun of solving the crime as the episodes unfold.

We're even drawn to tantalising characters we should be repulsed by, such as psychotic killers. Who didn't have a bit of a crush on the unhinged, sassy assassin Villanelle in the recent hugely popular BBC drama *Killing Eve*?

A good script writer will cleverly make us half love/half loathe a villain. That's because they create an authentic character. In reality, most of us are a mixture of light and shade – very few people are pure evil.

This special issue reveals how real-life serial killers become murdering monsters, why psychopaths don't necessarily carry out violent crimes, and how crime scene investigation really works (it's not quite like on TV). It also investigates how genetics is being used to solve cold cases, and how maths and AI can combat hackers and terrorists. Plus, discover the cutting-edge techniques that could one day be used to fight crime. Get ready, the robocops are coming...

Daniel Bennett, Editor



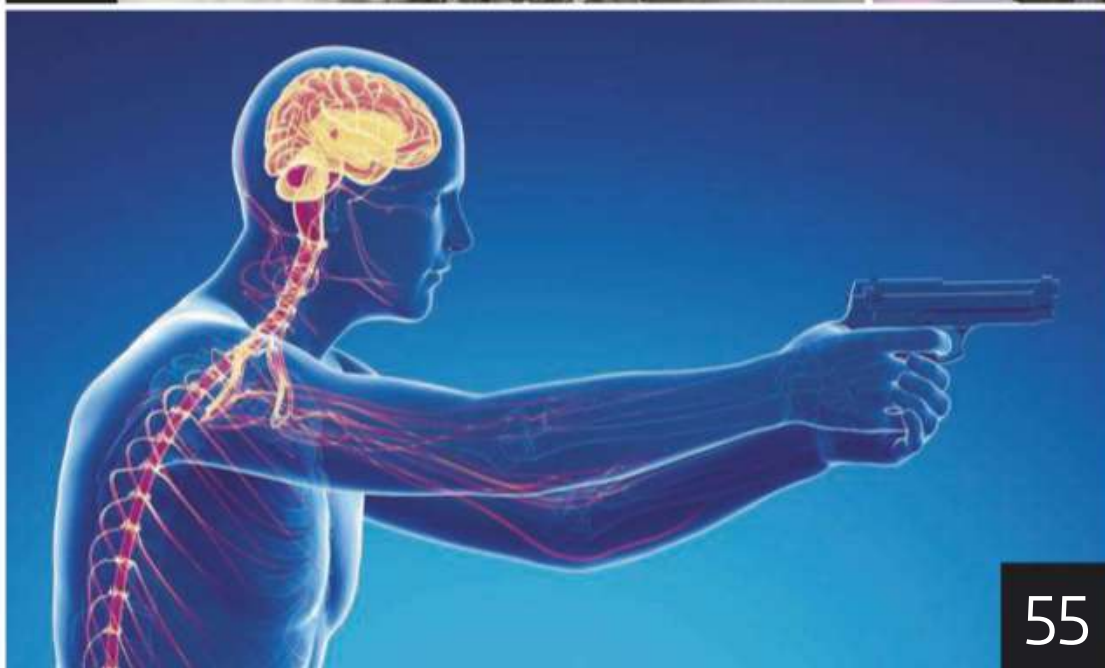
C O N T E N T



08



16



55

76



68



T S



06 Crime hotspots

Homicides, kidnaps, robberies, knife attacks

08 Forensic science

How investigators really solve crimes

14 The anatomy of a crime scene

The clues to look out for

16 Dead body farm

The scientists studying decaying corpses

22 DNA detectives

How genetics is helping solve cold cases

30 Genetic mugshots

How DNA is creating photofits

32 The psychopaths among us

Who around you fits the profile?

38 Psychopath test

Take the test to see if your boss is a psycho

40 Catching crooks

How profiling caught notorious criminals

48 How to get the truth

Tips from a former CIA officer

55 My brain made me do it

How brain injuries can create criminals

62 The new lie detectors

How MRI scanners can spot liars

68 How to beat hackers

The new techniques to foil malware

76 Maths to combat terrorism

How to prevent attacks before they happen

83 Robocops

The new police force taking to the streets

90 The future of fighting crime

Cutting-edge tech to beat criminals

98 My life scientific: Kerry Danes

The forensic psychologist on serial killers

CRIME HOTSPOTS

YOU MIGHT THINK YOU KNOW WHERE TO AVOID IF YOU DON'T WANT TO BECOME A VICTIM OF CRIME. BUT, AS THIS WORLD MAP AND STATISTICS SHOW, CRIMINAL HOTSPOTS CAN SOMETIMES SURPRISE YOU...

7. USA
15,883

3. MEXICO
20,762

8. COLOMBIA
12,782

1. BRAZIL
58,459

5. NIGERIA
17,843

LONDON

KNIFE CRIME

Total recorded*

2017/18	14,769
2016/17	12,106
2015/16	9,745
2014/15	9,691
2013/14	10,079

*SOURCE: Statista.com

ACID ATTACKS

Total recorded*

2017	465
2016	395
2015	255
2014	120
2013	131

*SOURCE: Metropolitan Police



ROBBERY

Per 100,000 people, 2015*

1	CAPE VERDE	1,051
2	ARGENTINA	1,020
3	CHILE	593
4	URUGUAY	566
5	PARAGUAY	317

*SOURCE: The UN Office on Drugs & Crime

CIVILIAN GUNS

Guns per 100 people, 2011*

1	UNITED STATES	88.8
2	YEMEN	54.8
3	SWITZERLAND	45.7
4	FINLAND	45.3
5	CYPRUS	36.4

*SOURCE: Small Arms Survey

KIDNAP

Per 100,000 people, 2015*

1	LEBANON	16.9
2	BELGIUM	10.1
3	CANADA	9.9
4	FRANCE	6.2
5	GERMANY	5.9

*SOURCE: The UN Office on Drugs & Crime

CRIME SCENE-DO NOT ENTER



HOW IT WORKS

FORENSIC SCIENCE

Scene-of-crime operatives in plastic overalls are a common sight on our TV screens. But what do they actually do?

WORDS: TOM IRELAND

WHAT IS FORENSIC SCIENCE? Any scientific process used as part of a criminal investigation is considered forensic science. This spans both the grim, grisly procedures of the autopsy room and the cutting-edge analysis of a crime scene. But it also encompasses the less glamorous, painstaking lab work of DNA profiling, fingerprint analysis and the uncovering of hidden digital files. There is even such a thing as forensic accountancy.

WHAT TECHNIQUES ARE USED TO SOLVE CRIMES TODAY?

The bulk of modern forensic work involves the analysis of DNA or fingerprints left at a crime scene. In murder cases, forensic autopsies help work out how a person died.

A range of more specialised and elaborate forensic techniques can be used to identify suspects in the most serious cases, such as tracking serial killers or terrorists. These methods include forensic ecology, where tiny traces of pollen or fungal spores can be used to tell where a suspect has been, or forensic entomology, where the presence of certain insects can help reveal how long a person has been dead.

As people spend more and more time on devices like smartphones and computers, so-called 'digital forensics' is playing an ever-greater role in criminal investigations, too. The growth in this field of forensic science also reflects the fact that there are now over four million CCTV cameras in the UK.

IS FORENSIC SCIENCE ANYTHING LIKE WHAT WE SEE ON TV?

Rarely. According to forensic scientist Prof Sue Black, who has advised a number of crime writers throughout her career, “There is an element of truth in TV crime, but also an element of fantasy – the work is often long, slow and laborious. But viewers quite rightly don’t want to see us doing our double-blind trials.”

Nathan Clarke, a professor of digital forensics and cyber security, says the depiction of tracking technology in spy movies, where security services miraculously enhance fuzzy images of suspects, is pure fiction. “In reality, you need someone to sit there and watch hours of video,” he says.

HOW DOES DNA PROFILING WORK?

Although 99.9 per cent of our DNA is the same in every person, the remaining 0.01 per cent is different enough to distinguish one individual from another.

Forensic DNA profiling looks specifically at highly variable stretches of DNA called ‘variable number tandem repeats’ (VNTRs). These are short sequences of genetic code that may occur tens or hundreds of times at specific points in a person’s DNA.

VNTRs are often located in parts of the human genome with little or no known function. Mutations in the genetic code here will not cause abnormalities, and so over many generations these sections of our genome have become hugely varied. And because unrelated people will almost certainly have different numbers of VNTRs in different places, they can be used to discriminate between two people.

DNA found at a crime scene is processed so that these sections can be compared to those from a sample swabbed from a suspect, or compared to a huge number of DNA profiles held on police databases. As well as helping to identify suspects, DNA profiling has helped prove the innocence of people incorrectly convicted, in some cases decades after the crime, and is often used to help identify victims, especially where people have been killed in large numbers or when their remains are badly damaged.

WHAT’S THE SMALLEST AMOUNT OF DNA FROM WHICH A SUSPECT OR VICTIM CAN BE IDENTIFIED?

As technology advances, scientists can process smaller and smaller samples to develop a DNA profile. Modern techniques can ‘amplify’ tiny amounts of DNA from minute traces of any material that contains fragments of tissue or cells, such as blood, semen, saliva, urine, faeces, hair, teeth or bone. ‘Low-level’ or ‘touch DNA’ can sometimes even be collected from a few skin cells left behind after a person has touched an object or victim.

With a full sample and the latest DNA profiling techniques, investigators are able to generate a ‘match probability’ of up to one in a quintillion (1x 10¹⁸). The chance of a random person in the population having that DNA profile is infinitesimally small.

IF A SUSPECT’S DNA IS FOUND AT A CRIME SCENE, WILL IT ALWAYS LEAD TO A CONVICTION?

Not necessarily – there are all sorts of innocent reasons why a person’s DNA could be at a crime scene or on a body. And even when DNA found at a crime scene is clearly that of the perpetrator, the police still need to find a match – if the murderer is not already a suspect, and their DNA profile is not on file, the evidence is effectively useless.

However, in such cases a person’s own family can land them in it. A serial killer known as the Grim Sleeper, who killed at least 10 people in Los Angeles between 1985 and 2007, eluded police for decades, despite them having a sample of his DNA.

A suspect was finally apprehended when his son was arrested for weapons offences. The son gave a regulation DNA sample, which partially matched the DNA profile found at all of the Grim Sleeper crime scenes, which led the police to investigate his relatives. Police

Police posed as waiters to get the father’s DNA from a pizza slice, and found that it matched the crime scene DNA

ABOVE: Fingerprints have been used to identify criminals since the 1890s

RIGHT: Lonnie David Franklin Jr was arrested for the Grim Sleeper murders in 2010

GETTY X2

JARGON BUSTER

DNA PHENOTYPING

Something of a holy grail for forensic scientists, DNA phenotyping creates a 'photofit' image based on a DNA sample alone. But the technique is still being developed.

DNA PROFILING

A person's DNA profile is not simply their entire DNA sequence, which is billions of letters long. Instead, profiling compares the DNA in around a dozen highly variable stretches of the human genome.

ENTOMOLOGY

The study of insects. Forensic entomologists can work out the time of a victim's death by studying the types of insects feeding on their corpse.

LOOPS, WHORLS AND ARCHES

These are the classic patterns made by the ridges of skin in a fingerprint. Fingerprints are still commonly used to identify suspects today.

MATCH PROBABILITY

This complicated calculation essentially gives the probability of a forensic match occurring by chance – for example, the likelihood that your DNA matches some DNA found at a crime scene which is not actually yours.

PALYNOLOGY

The study of pollen and other tiny biological spores, which can link a suspect to a crime scene. Pollen is useful as it's very easy to pick up but very hard to remove from clothing, and is normally completely invisible to anyone other than an expert.

posed as waiters to get the father's DNA from a pizza slice, and found that it matched the crime scene DNA.

CAN DNA EVIDENCE BE FAKED?

Although DNA profiling is an excellent way to distinguish between individuals, it is still not immune to falsification, errors or manipulation. In 1992, a doctor and rapist called John Schneeberger evaded justice by injecting other people's blood into his arm just before his DNA was sampled by police. He was found guilty when forced to take another test years later.

It's also possible, although extremely rare, for a person to be a 'genetic chimera', meaning that they have cells in their body with different DNA from the rest of them.

WHY DO FORENSIC SCIENTISTS STILL USE FINGERPRINTING?

With fingerprints, police can often use their own in-house specialists rather than call on external forensic scientists. The digitisation of fingerprint records means a photograph of a fingermark can be sent from a crime scene and compared to a database almost in real-time.

According to the Fingerprint Society, fingerprints remain the number one ID metric for crime scenes in the UK, accounting for the identification of well over 100,000 suspects in 2012. Prints can also help indicate what someone was doing or how they entered a building – for example, if they are found leading up to a broken window or in a grip figuration on a weapon. And unlike DNA, it's hard to plant a fingerprint at a crime scene.

HOW ACCURATE IS IT?

Fingerprints may be considered an 'older' forensic technique, having first been used in the 1890s, but the technology behind them is continuously being improved. As well as the well-known method of 'dusting' for fingerprints at the scene, forensics teams can also use chemical reagents and lasers to reveal extremely faint prints.

Even more sensitive tools can be deployed if objects are taken back to the lab. One method involves gold or silver particles being placed ➔



WHAT WE STILL DON'T KNOW

WHO OWNS OUR DNA?

Police forces have been compiling large databases of DNA profiles for years, sometimes from people they've arrested but then released. Having the DNA profile of everyone in the country is a detective's dream, but others say it turns everyone into a suspect. With DNA-testing companies and the NHS also collecting DNA samples en masse, there's no easy answer to the question of who actually owns your genetic code, or what they can do with it.

HOW TO POLICE THE DIGITAL WORLD

Government security agencies are locked in a battle with technology giants over how to access evidence they say is crucial to preventing terrorism. Amazingly, even the FBI's digital experts can't unlock encrypted iPhones without the help of Apple. Even more worrying for security services is the burgeoning art of digital steganography – hiding secret messages within seemingly benign files such as holiday photos.

CAN DNA GIVE US AN IDEA OF WHAT A SUSPECT LOOKS LIKE?

Scientists have been able to map how certain genes are linked to certain facial features, but this relationship is complex. A DNA sample is also unlikely to ever be able to tell us whether someone is overweight or suntanned, as these are environmental, and not genetic, characteristics. Besides, you can always put on glasses or (if male) grow a beard.



The FBI wants Apple to unlock a terrorism suspect's iPhone, but Apple refuses

Blowflies are usually the first insects to invade a dead body



with a sample in a vacuum; the metal will settle on the faintest of marks.

IS EVERYONE'S FINGERPRINT REALLY UNIQUE?

The underlying patterns of ridges on people's digits are determined genetically, but the way individual ridges divide and break is dependent on conditions in the womb and the movement of the developing foetus. Even the fingerprints of identical twins will be different, while their DNA will be the same.

Pollen and fungal spores are important as they are picked up easily but not easily shed, even from clothing and footwear that's been washed

WHAT ELSE MIGHT POLICE LOOK FOR AT A CRIME SCENE?

Criminals often wear gloves while committing premeditated crimes, but they can't float in and out of the crime scene, so footprints can be crucial. While footwear can't definitively identify an individual, knowing the exact model of shoe the perpetrator wore is still very useful intelligence when looking for a suspect.

In more serious crimes, forensic ecologists will look for traces of biological material that can link a suspect to a certain area, such as the type of woodland where a body has been found. Pollen and fungal spores are especially important as they are picked up easily but not easily shed, even from clothing and footwear that's been washed. But suspects are likely to have walked through many types of soil, mud or vegetation before and after being at a crime scene. It all adds up to a huge headache for those trying to analyse and compare all the biological material found on the suspect. The rarer the pollen or spore that forensics can match, the more credible the case.

A good example is also the first ever example of forensic ecology. In 1959, a man was murdered



Forensic science isn't as glamorous as TV suggests

EXPLAIN IT TO A FRIEND

1 IT'S NOTHING LIKE ON TV

Forensic science, especially DNA analysis, can often involve tedious laboratory work – something that TV programmes usually neglect to show. For forensic evidence to hold up under scrutiny in court, every stage of the process – collection, handling, storage and analysis – must be conducted to impeccable scientific standards.

2 PRINTS AND PROFILES

DNA and fingerprints are the most commonly used forensic evidence in criminal investigations. Apart from identical twins, no two people have the same DNA, and DNA samples are compared at points where the human genome is known to be incredibly varied. Fingerprints are still used, though, as they're cheaper to process and more likely to indicate what someone has been doing.

3 EXTRAORDINARY EVIDENCE

A huge range of materials can be collected and analysed to match a suspect to a crime scene. The more unique or rare the material, the more credible the case against them. It can be anything from pollen grains and mud to chemicals and even bacteria.

while travelling down the river Danube in Austria, but a body had not been found. Mud on the suspect's shoes contained a type of pollen from ancient hickory trees. Scientists concluded this could only have come from vegetation growing on exposed Miocene-age rocks, and the only place such soil had developed was a small section of the river 20km north of Vienna. Presented with this theory, the suspect confessed and took police to the body – exactly where the scientists had predicted.

Other techniques often seen on TV, such as blood spatter and ballistics analysis, may give detectives an idea of what happened at a crime scene, but rarely help find the perpetrator.

WHAT CAN FORENSIC TEAMS LEARN FROM HUMAN REMAINS?

In the first 72 hours after death, a pathologist is usually able to provide a reasonably accurate determination of the time and cause of death. If a person has been dead for longer, forensic entomologists may be called on to estimate the time of death, based on the number and type of insects feeding on the corpse. This method can be used to determine a period of hours, weeks or even years since death.


Blowflies are almost always the first insects to arrive and lay eggs on a corpse, as they are mobile, common and able to smell death from up to 10km away. Eventually other families of insects are attracted to the body, such as beetles.

See page 16. For more heavily decomposed or damaged remains, forensic dentists can match remnants of teeth to known dental records, or even use what they find to draw conclusions about the victim's age, size, gender, race and socioeconomic status.

WHAT IS CURRENTLY BEING DEVELOPED AT THE CUTTING EDGE OF FORENSIC SCIENCE?

Forensic scientists can use anything to link a suspect to a crime scene, as long as they can prove the samples are unlikely to match by chance. In the US, scientists have looked at the atomic structure of fragments of glass to prove it was from the same sheet of glass as that found broken at a crime scene.

Pioneering techniques that mix digital forensics with anatomy are also now being used to identify people from small areas of their body seen in photos or videos. Features such as vein patternation or knuckle marks can identify suspects from images showing only small areas of their hands or arms. Grimly, this is likely to be used in cases involving sexual abuse.

As our understanding of DNA improves, we are starting to be able to create a photofit-style image of a suspect solely from DNA evidence (see page 30). However, such 'DNA phenotyping' can't predict many aspects of how a person looks, such as whether they have a beard. 

Tom Ireland is a science writer and editor of *The Biologist*, the magazine of the Royal Society of Biology.



Catching History's Criminals: The Forensics Story on the BBC Store: store.bbc.com/catching-historys-criminals-the-forensics-story



ANATOMY OF A MODERN CRIME SCENE

A man has been found murdered in a suburban home. The killer may have got away, but forensic scientists have plenty of evidence to pore over...

1 FINGERPRINTS
Prints can be recovered from surfaces. Their position helps detectives sequence events.

2 INSECTS
Insects on the body can help to determine when the victim died. Blowflies and then maggots arrive first, followed by beetles.

3 SALIVA
There may be visible bodily fluids, but DNA can be collected from less obvious sources, such as a drinking glass.

4 VEGETATION
Pollen and spores from plants and fungi can stick to clothes or car tyres, linking suspects to a precise location.

5 FOOTMARKS
Forensics can recover a footmark that's almost invisible to the eye.

6 DIGITAL FOOTPRINT
With our smartphones, travel cards and online activity, most of us now leave a digital trace that can be easily followed.

BBC
RADIO

4

Listen to *The Life Scientific* with a forensic entomologist discussing how her knowledge of insects helps solve crimes
bbc.in/2SNRkxc



Students excavate
a corpse at the
body farm at Texas
State University

ON THE BODY FARM

Corpses can tell you a lot. Just like language, decomposition is dependent on location. Which is why some researchers say we need to start studying the dialect of decay in the UK

WORDS: ROB BANINO

Dr Anna Williams wants to watch you rot. It's nothing personal; it's for science, specifically the science of taphonomy, which is the study of decay and fossilisation. By monitoring how corpses decompose, she hopes to increase our understanding of the subtleties of the process and improve the accuracy with which we can locate and identify dead people, and determine their time of death.

In order to do this, Williams, a forensic anthropologist at the University of Huddersfield, wants to establish a human taphonomy facility in the UK. There are already nine such facilities – colloquially known as ‘body farms’ – around the world: seven in the US, one in Australia and another in the Netherlands. So why do we need one here?

“What we know about decomposition has come out of the American facilities,” explains Williams. “Before the first one opened in 1981,

we really didn't know very much about how bodies decompose in different conditions. The research that's been going on since then has really boosted our knowledge.

“And one of the things we've learned is that decomposition is incredibly dependent upon local conditions: the surrounding temperature, rainfall, humidity, soil type, ecology, insects, scavengers. So, the information coming out of the existing facilities is very useful, but it's not directly applicable to forensic cases in the UK.”

In short, people in the UK don't decay in the same way as they do elsewhere. In fact, people don't always decay the same way in the same country. And we wouldn't know that if it wasn't for the pioneering work of forensic anthropologist Dr William Bass.

Bass founded the first human decomposition research facility at the University of Tennessee after recognising how misleading the decay process could be. The realisation came in 1977 after local police contacted Bass and asked ➔

FBI PHOTO LIBRARY ILLUSTRATION: MICHAEL HADDAD

Listen to an interview with Dr Anna Williams on the *Science Focus* podcast. Visit sciencefocus.com/sciencefocuspodcast

him to examine some human remains they'd found in a disturbed grave. The corpse's head was missing, but based on the remaining flesh and bones it was originally determined that the remains belonged to a white male in his mid-to-late 20s who'd been dead for about a year.

However, Bass's examination revealed something astounding: the corpse was older than everyone thought. A lot older. It was actually the body of the Confederate soldier, Colonel William Shy, who'd been dead for over a century. The remains were so well preserved because they'd been embalmed and buried in an airtight coffin. What the police had found wasn't a killer's attempt to hide the body of a recent victim but the remains of a corpse that had been dug up by graverobbers. The confounding nature of Colonel Shy's corpse led Bass to an epiphany: we needed a far better understanding of human decomposition and the factors that affect it. We needed to study it closely, and to do that we'd need decomposing bodies and somewhere to watch them fester.

That place ended up being a 10,000m² fenced-off wooded area in Knoxville, Tennessee – the outdoor decomposition research facility of the University of Tennessee's Forensic Anthropology Center. In the 37 years since it opened, Bass and his colleagues have scrutinised the decay of thousands of cadavers in various states: buried, unburied, whole, dismembered, hidden in car boots, wrapped in carpet and entombed in concrete. And the contribution they've made to our ability to locate and identify human remains, and more accurately infer their time of death, is unquantifiable.

SPEEDING UP THE ROT

The progress made at Tennessee inspired other US universities, like Texas State University, to build on Bass's example. Dr Daniel Wescott is the current director of the Forensic Anthropology Center at Texas State (FACTS), which opened in 2008. "We have lots of graduate students researching different aspects of decomposition, such as what happens if you wrap a body in a specific material," he says. "Tarps and carpets tend to accelerate the rate of decomposition as they retain heat and moisture, and provide protection for the insects so that they feed a

little faster. Typically, wrapping a body will accelerate the decomposition but it also depends on if it's buried or not."

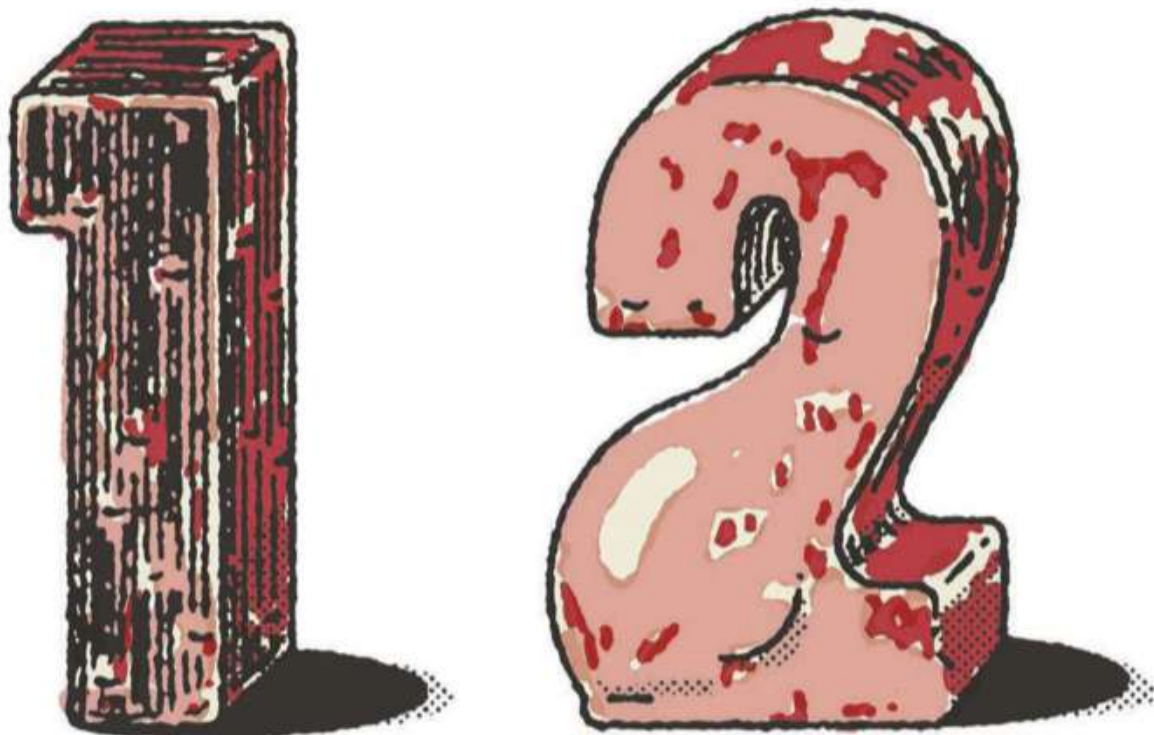
Until now, searches for missing bodies have relied on manpower, specially trained sniffer dogs and ground-penetrating radar devices. But, as Wescott explains, FACTS is testing ways to locate corpses using drones: "In the early stages of decomposition you've got a lot of chemical reactions going on, you've got bacteria proliferating, you've got maggot activity... and all that generates heat. We can use infrared cameras on the drones to pick up that heat. "Later on, a skeleton's not going to give out heat, but we can use near-infrared photography to pick up what's called a 'cadaver decomposition island'. This is what you get when the fluids seep out of a decomposing body into the surrounding soil. We can pick up the areas of enriched soil because it reflects light differently."

RIGHT: Students at Texas State University clean bones after the soft tissue has decomposed. The bones will be sent to the university's permanent skeletal collection

FAR RIGHT: Dr William Bass pioneered body farms as a way to increase our knowledge of decay

BREAKDOWN

Left unburied and uncovered, here's what happens to a body...

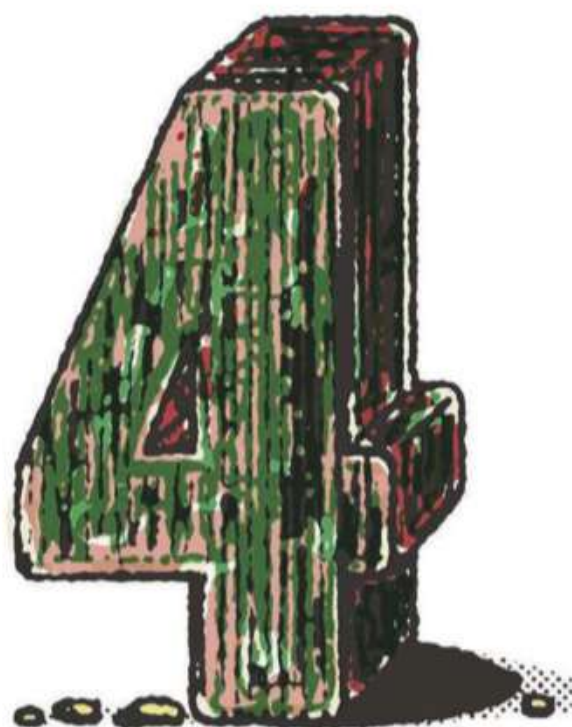


The fresh stage can last a few days to a week. Rigor mortis initially sets in and cells break down as the lack of oxygen and nutrients prevents them from replenishing themselves.

When bacteria in the gut can no longer be kept in check, they start to reproduce and feed on the body. This produces gas that causes the abdomen to bloat.



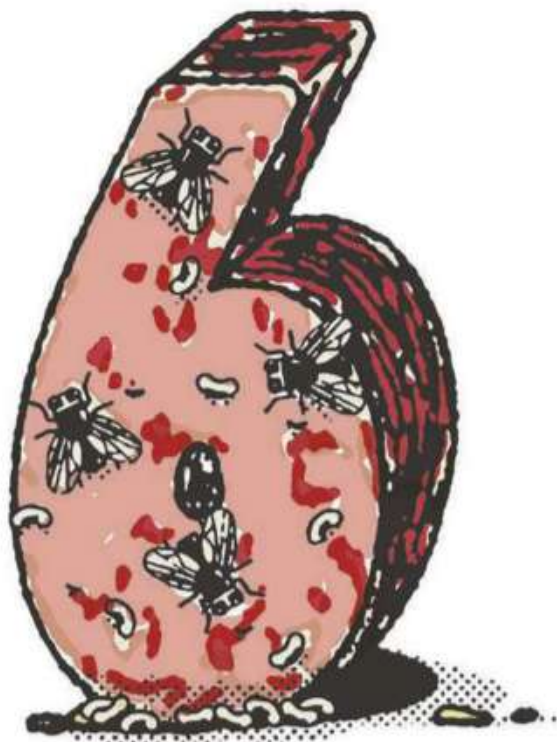
Gas building up increases pressure within the body, pushing fluids in between the layers of skin and causing the outer layers to slough off.



With no oxygen to bind to, haemoglobin in the blood binds to sulphur instead, filling the arteries and veins with a greenish-black substance. This gives the flesh an appearance known as 'marbling'.



Increasing pressure forces the body's fluids and liquefied organs out of any available orifice. Eyeballs can be dislodged and bodies have even been known to explode.



Chemicals released by the body attract flies, which lay eggs in and around the orifices. Soon after, maggots hatch and begin feeding on the body's flesh and organs.



Other insects, such as beetles, are attracted to the body, as well as small birds looking to feed on them. Local scavenging animals will also appear to pick the flesh off the bones.



The final stage is skeletonisation, when the soft tissue is fully lost. Wind, rain, erosion and abrasion take over and the bones are disarticulated over the following months and years.

But as useful as this research is, no one can pretend the climate in the US is anything like that of the UK. “Environmental variables have a big influence on the rate at which a body decomposes. So, when you’re talking about trying to calculate how long somebody’s been dead, the basic principles that come out of Texas apply but the specific rate probably wouldn’t apply to Europe,” says Westcott. Which brings us back to Williams and the need for a human facility in the UK.

Williams has already taken steps to advance the understanding of decomposition in the UK by opening an animal taphonomy facility in Cranfield University in 2011. But recent studies have shown that the pigs, rabbits, mice, sheep and deer used in such labs aren’t suitable analogues for humans because they have different gut bacteria, medical conditions, diets and lifestyles. To put it another way, pigs don’t smoke, get diabetes or overindulge on fast food, alcohol or drugs, all of which can affect the way a body breaks down. And if the information generated using animals isn’t comparable to humans, aside from the doubt it casts on any research, it can also be more easily undermined if it’s

Animals aren’t suitable analogues. Pigs don’t smoke or get diabetes, which can affect how a body breaks down

used in testimony during a trial.

Hence the need for a human facility in the UK. But in order to get one, Williams needs to raise the funding for it (to the tune of about £1m), find a suitable site and generate support from the UK’s universities, the Human Tissue Authority and the public. All of which is a tricky proposition given the delicate nature of

what Williams intends to study and people’s perceptions of how she might study it. But there are ways to mitigate any offence an outdoor lab containing rotting corpses may cause.

FORENSIC CEMETERY

“One thing that we might do is try a staggered approach so that we start with a facility more like the one in Amsterdam, which is

called a ‘forensic cemetery’ because the bodies are buried,” she says. “You can’t see the bodies as they’re not on the surface and that’s perhaps less objectionable, more readily acceptable.”

In such a scenario, monitoring equipment and possibly even viewing windows would be installed underground to study the cadavers as they decompose. But it may actually be the perception of the public’s attitude towards such a facility that’s mistaken.




At Texas State University, some corpses are kept inside cages to protect them from scavengers

A survey carried out by Williams suggests people are in favour of a human taphonomy facility in the UK, and she's already getting offers from people wishing to donate their bodies and has support from the Home Office. Were such a facility to eventually open here, aside from the research benefit it could provide, Williams believes it would also enable more people's dying wishes to be granted.

"Lots of people want to donate their bodies to anatomy schools for teaching and dissection, but often they're turned away because they have conditions that mean they're unsuitable. A taphonomy facility would turn away fewer people because it wouldn't matter what state their body was in or what conditions they had."

In an ideal world, Williams hopes that donors will not only be able to choose what sort of research their body is used for, but also what happens to their remains afterwards.

"[If we get one in the UK] there'll be a lot of setting up," says Williams. "It'll probably be months before we get the first experiments underway because there's so much testing to do. We've got to find out what everything is like – the vegetation, soil type, humidity, temperature, even the number of worms, birds and snails – before we put the bodies in."

So it seems there's still a lot of work to be done, even if a UK facility does get the go-ahead. 

Rob Banino is a Bristol-based writer and editor, specialising in science, technology and cycling.



Watch a short video about Australia's body farm at bit.ly/body_farm

OTHER THINGS TO DO WHEN YOU'RE DEAD

Donating your body to medical science is one way to make yourself useful after death. But here are some less run-of-the-mill options...

CRASH CARS

Car manufacturers like to show the efficacy of their vehicles' safety features with slow-motion videos of dummies getting thrown about during a collision. What they're less keen to publicise is that they've probably put dead bodies through the same tests to see how the impacts affect their internal organs.



PUT ON A SHOW

Body Worlds exhibitions feature real corpses and organs that have been preserved through plastination, a technique invented by Dr Gunther von Hagens. If you're willing to go on display after your bodily fluids and soluble fat have been replaced by liquid plastic, you could donate your body to the Institute for Plastination.



GROW A TREE

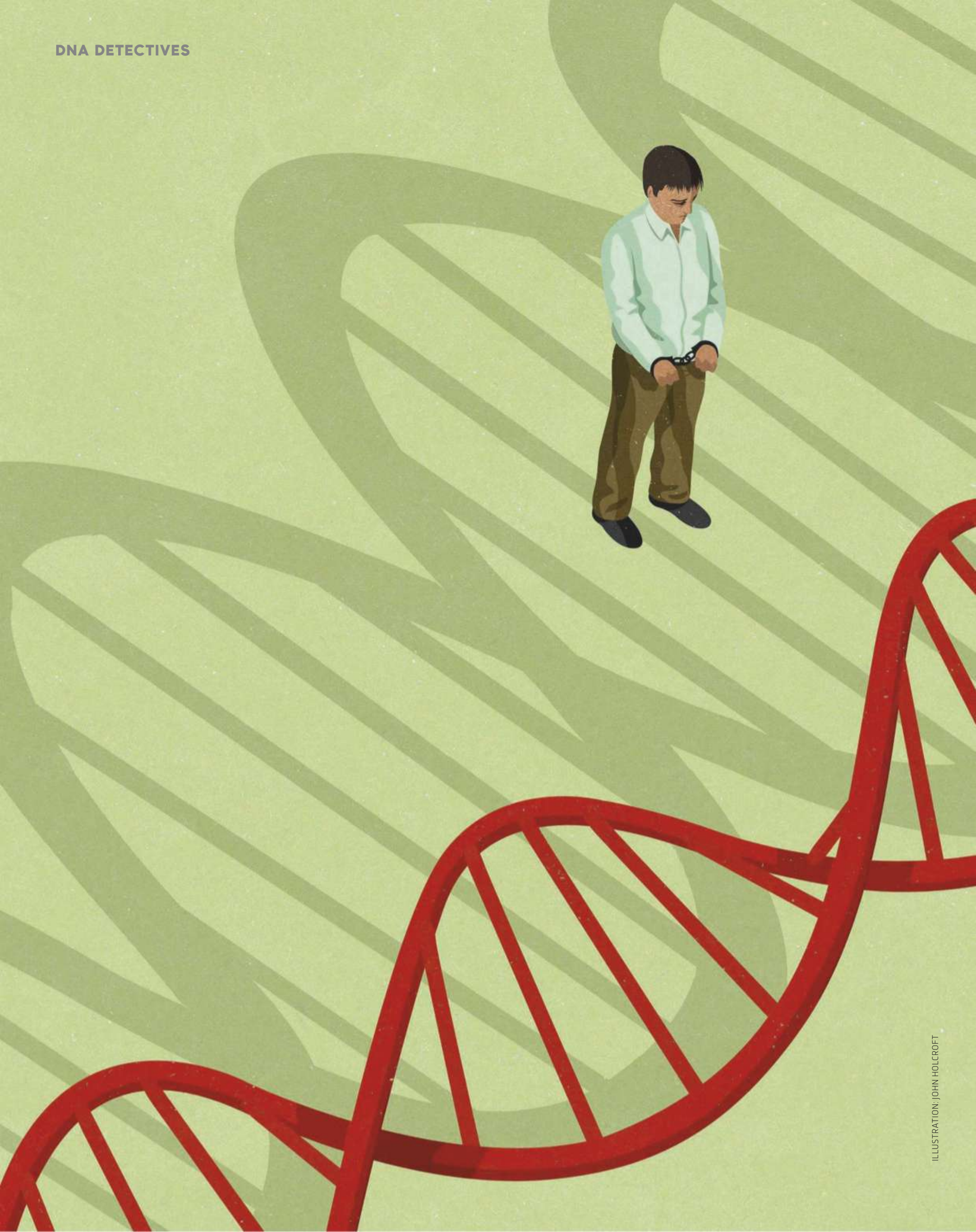
You can still make yourself useful after you've been cremated, depending on what happens to your ashes. Scattered on soil, they'll act as a general fertiliser, but if you want something more specific you can have them added to a Bios Urn, a biodegradable container packed with soil and used for tree seed germination.

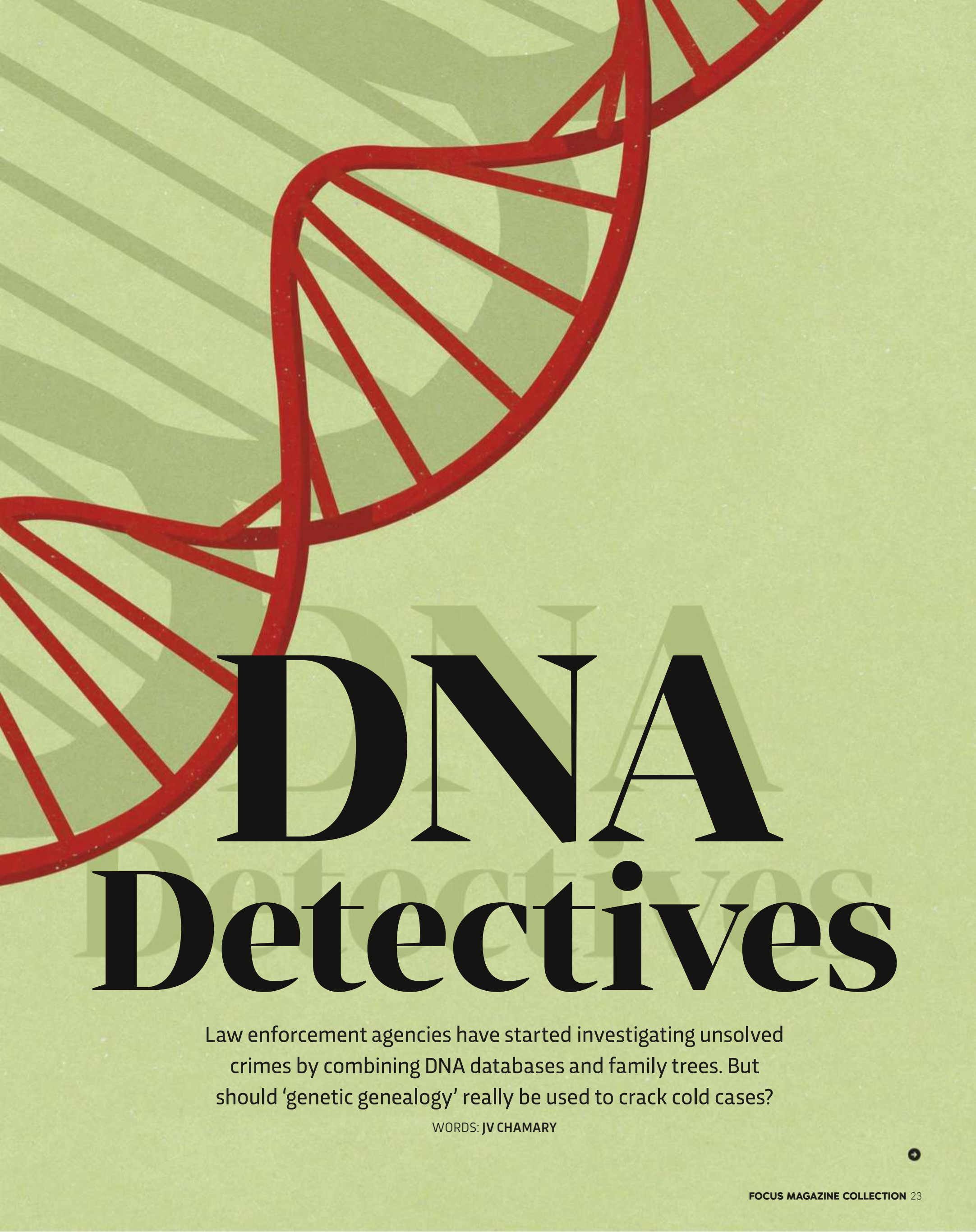


RELEASE A RECORD

An audio recording of your voice or music that held a special meaning for you is one way that loved ones can treasure your memory. If, however, you'd like the keepsake to bear slightly more of your physical presence you can get andvinyl.com to press your ashes into the vinyl on which your voice and music is printed.







DNA Detectives

Law enforcement agencies have started investigating unsolved crimes by combining DNA databases and family trees. But should 'genetic genealogy' really be used to crack cold cases?

WORDS: JV CHAMARY



From 1976 to 1986, the residents of California were terrorised by a masked man who raped at least 48 women and murdered a dozen people. His carefully planned attacks suggested military training, but after three decades, the East Area Rapist – also known as the Golden State Killer – seemed to have got away with his crimes. The case went cold.

Then on 25 April 2018, law enforcement officials announced that they had arrested Joseph DeAngelo, a 72-year-old Navy veteran and former cop. Investigators explained that semen samples from crime scenes had been used to produce the perpetrator's DNA profile and search an online database for potential relatives. The list of matches was then used to build a family tree that led to DeAngelo.

While catching killers using 'genetic genealogy' might sound like an obvious idea, it is not straightforward. "Humans are really similar genetically: if I compared my genome to yours, we'd be 99.99 per cent identical," says Prof Graham Coop, a population geneticist at the University of California. "But there are positions in DNA which are variable between individuals."

Modern genetic tests read the letters of DNA at a selection of positions across the human genome to generate a profile of genetic variants. These single-letter differences represent DNA regions that often vary among people, called 'single nucleotide polymorphisms' or SNPs (pronounced 'snips').

Personal genomics companies like 23andMe and Ancestry offer 'direct-to-consumer' DNA tests that read about 700,000 SNPs. Those variants generate a profile that claim to reveal



TOP ROW: Joseph DeAngelo, the Golden State Killer, during his years as a police officer, and (right) a 1976 police sketch of the killer

ABOVE: DeAngelo was finally arrested in 2018. His case is ongoing

your family history, ethnic background and susceptibility to disease.

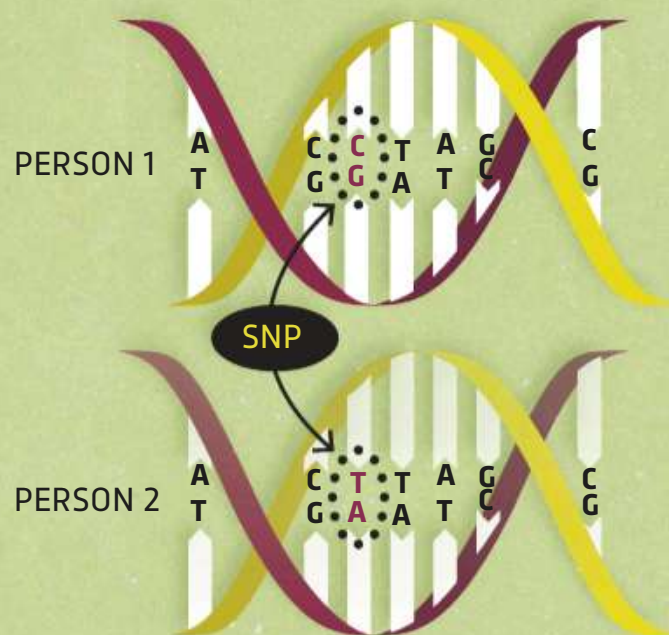
Genealogists who want to study a family tree in detail can upload DNA profiles to a site like GEDmatch, which compares SNPs shared by two people to calculate their genetic similarity. The GEDmatch (GEnealogical Data match) website stores public profiles uploaded by its one million users. Unlike private databases run by DNA-testing services like 23andMe, GEDmatch can be searched by anyone who registers for access, which is how investigators found DeAngelo. "Finding these genetic matches is easy," says Coop. "The actual work the investigators did is the hard part."

Catching the alleged Golden State Killer was a watershed moment for how combining databases and family trees can help crack cold

If police want a DNA sample, they need your consent or a search warrant – at least in principle

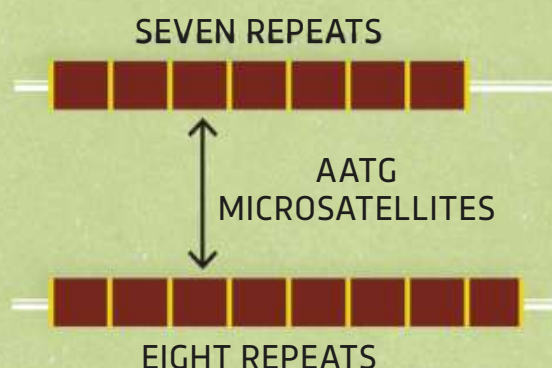
GENETIC VARIANTS

The human genome is our complete set of 23 chromosomes. It's made from DNA and is over three billion letters long. The differences between individuals can be found at locations that commonly vary between us – genetic variants. Here are three different types that are used to compare people



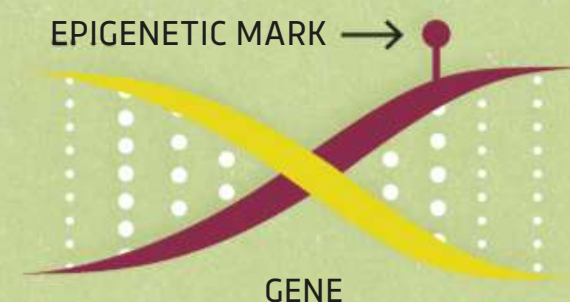
SINGLE NUCLEOTIDE POLYMORPHISMS

Nucleotides, the building blocks of DNA, include one of four chemical letters: A, C, G or T. The most common genetic variations in humans are 'single nucleotide polymorphisms', known as SNPs. These are positions in DNA where two people might carry the same letter, or different letters. There are 10 million SNPs across the genome and the vast majority don't affect how your body works. Personal genomics firms like 23andMe offer tests that read SNPs to generate a DNA profile, which is compared against other profiles in their databases to indicate your family history, ethnic background and risk of inherited diseases.



MICROSATELLITES

Approximately 3 per cent of the human genome is composed of microsatellites, also known as 'short tandem repeats' (STRs). Each microsatellite is a repeating unit made up of one to six DNA letters. The number of repeats varies among people. For example, at any given location you might carry seven copies of the unit AATG, whereas someone else might have a variant with eight copies. The FBI's Combined DNA Index System (CODIS) database has profiles created from 20 positions. Such profiles are also used in forensics and paternity testing, comparing two individuals to see if they share the same number of repeats at each location.



EPIGENETIC MARKS

While they aren't technically genetic variants, epigenetic marks do contribute to the differences among people. Epigenetic marks are chemical modifications to DNA and its associated proteins that can influence whether genes are switched on or off, and therefore affect the behaviour of our cells. Some marks are attached and removed during the course of development, others are the result of lifestyle choices, such as smoking. Scientists can now read where marks highlight sentences on DNA, meaning we could soon take tests that create epigenetic profiles, which could be used in forensics to identify a smoker, for instance. Such personal epigenomic reports could reveal info about physical features.

cases. "That opened up the potential of what we would be able to accomplish," says genetic genealogist CeCe Moore, who previously focused on cases of unknown parentage, like adoption.

Moore now heads the new genetic genealogy unit for Parabon NanoLabs, a firm that provides forensic services to law enforcement agencies. After DeAngelo's arrest, Parabon uploaded more than 100 DNA profiles to GEDmatch, with its permission (investigators didn't ask before uploading the Golden State Killer's profile).

Moore's first case was a double murder in Washington State. The male killer's DNA profile was uploaded on a Friday and by Saturday she had a list of matches for building a family tree that led to a marriage that produced three daughters and one son. By Monday, she had a name for the police: William Talbott II.

Parabon now offers a genetic genealogy service to any agency, not just existing customers. With enough human resources, it could help crack hundreds (maybe thousands) of cold cases. If DNA is available, the approach could be applied to other infamous criminals, such as the Zodiac Killer, who murdered at least five people in the late 1970s and taunted police with letters that might carry traces of saliva.

ETHICAL CONCERNS

While it may seem that catching bad guys can only be a good thing, there are legal issues to consider, especially privacy concerns for people whose DNA is stored in a database. What if your profile is downloaded and leads to identity theft? Or genes associated with disease or ethnicity are used to discriminate against ➔

you when trying to get a job? Such scenarios could occur in future.

For Americans, the issue centres on whether you're entitled to a reasonable 'expectation of privacy' under the United States Constitution. "One of the biggest privacy protections is the Fourth Amendment, which protects individuals against unreasonable searches and seizures," says Dr Natalie Ram of the University of Baltimore School of Law.

If police want a DNA sample, they need your consent or a search warrant – at least in principle. In practice, they can follow you until you discard DNA in a public place – such as saliva on a coffee cup – then lawfully grab a 'surreptitious sample' (that's how police obtained

DeAngelo's DNA). It's possible because you waive your rights to property when it's been thrown away, the 'doctrine of abandonment'. Even uploading your profile to a database might be considered 'abandonment' under US law: in the 1970s, the Supreme Court said the Fourth Amendment didn't cover data voluntarily shared with a third party.

What about here? For now, UK law only applies to DNA profiles for convicted criminals. "Our National DNA Database is quite well-regulated in terms of who gets on it, who's allowed to access it," says Prof Carole McCartney of Northumbria University. "But there's no rules about private companies – it will come down to their terms and conditions." The European Union's recent

DNA testing is helping to catch more criminals than ever, but the wider ramifications need to be considered

HOW IT WORKS

Identifying the perpetrator of a crime using DNA databases and family trees

PERPETRATOR

USER

1

COLLECTING SAMPLES

Crime scene investigators collect biological material such as blood, semen, hair or skin. The DNA molecule decays over time and has a 521-year half-life under ideal conditions (-5°C), but degrades quickly when exposed to heat, light, water and air. Whether DNA stays viable also depends on how well it's stored. The oldest DNA recorded was found in Greenland ice, and was estimated to be between 450,000 and 800,000 years old.

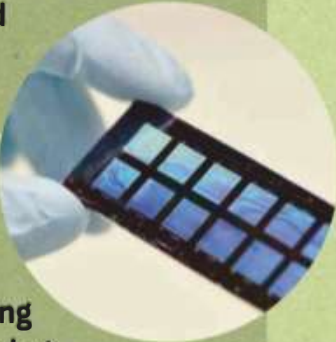
2

TESTING DNA

DNA molecules are cut into fragments and added to a 'genotyping chip'. Genotyping chips are covered in an array of 700,000 microscopic wells, each containing a probe that will match a genetic variant, which may or may not be present in the DNA sample. If a fragment matches, it can be labelled with one of several fluorescent dyes that enables a computer to read each associated DNA letter.

When someone orders a £100 DNA testing kit from direct-to-consumer genomics companies like 23andMe, Ancestry or MyHeritage, they spit into a collection tube or take cells from a cheek swab, then post the sample to the company. After four to eight weeks, they log into their account for a report.

Genomics companies use different genotyping chips, depending what that company believes are the most informative genetic variants. Most companies allow users to download a text file showing their genetic variants or 'genotypes', which are also uploaded to GEDmatch, a searchable genealogy website.



GENETIC



General Data Protection Regulation (GDPR) law gives citizens greater control over how their information is handled, but McCartney thinks it's accepted that the police can use genetic data. British police could search GEDmatch profiles to track down suspects with American relatives.

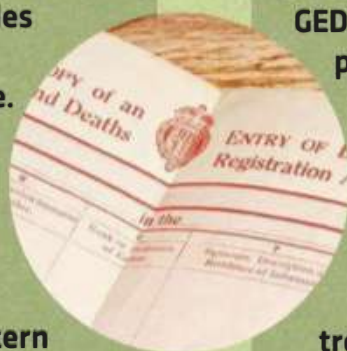
Over-reach can happen through 'function creep' – when the use of new technology (like DNA databases) is sneakily stretched beyond its original purpose. This can cause an invasion of privacy, as illustrated by the National DNA Database, which initially added people who had been arrested but didn't remove them after release. The case ended up in the European Court of Human Rights and led to the Protection of Freedoms Act. The danger is compounded by ➔

3 SEARCHING DATABASES

The DNA profile of genotypes for one person, the criminal, is compared against the profiles from other people in GEDmatch's public database. Each genotype is a single DNA letter or 'single nucleotide polymorphism' (SNP) at one of 700,000 positions that vary in the human population. The pattern and number of SNPs shared by any two people is used to calculate their genetic similarity.

A database search is unlikely to return matches with high similarity. As a person inherits half their DNA from each parent, they're 50 per cent similar to their mother and father, 25 per cent to a grandparent. For each generation since cousins last shared a common ancestor, similarity is reduced by a quarter. So first cousins share roughly 12.5 per cent of their DNA, second cousins 3.125 per cent, etc.

Going back to fifth cousins (sharing great-great-great-great-grandparents) the overlap is just 0.05 per cent – effectively unrelated.



4 BUILDING TREES

The chances of matching many first or second cousins in a database the size of GEDmatch, which contains one million DNA profiles, is extremely low. But there's a high probability that you'll find tens or even hundreds of third and fourth cousins, as there are enough profiles and their DNA is still similar enough to be identified by genetic similarity.

Genetic genealogists build a family tree by applying traditional techniques to database information, such as the names of two people and their DNA similarity. This includes finding records like census data, newspaper obituaries and birth and marriage certificates, and interviewing living relatives. Nowadays it also involves figuring out relationships via Facebook and other social networks.

Once links between cousins are confirmed, a genetic genealogist works backwards to find where the separate branches of a tree are connected at their long-dead ancestors. Recent twigs of the family tree (living relatives) are then added by building forwards ('reverse genealogy'), which can sometimes succeed in 'triangulation' – when two distant branches intermarry.



5 FINDING SUSPECTS

Police, FBI and other law enforcement agencies use conventional investigative methods before arresting a suspect. For the Golden State Killer, investigators only had a list of third cousins (sharing great-great-grandparents and under 1 per cent genetic similarity) so they had to use an extensive process of elimination (the offender was about 5'9" and 75kg, for example) to narrow it down.

Identifying a suspect requires putting all the pieces of a puzzle together. In Moore's first genetic genealogy case, GEDmatch had a list of

possible relatives that included two distinct matches, each with a 3 per cent similarity to the killer's DNA. This suggested they were second cousins from different branches of the family tree, enabling Moore to identify Talbott II by triangulation.

misplaced trust in the forensic process, which is vulnerable to errors: investigators can cause contamination while collecting DNA, or mix up samples while processing. Despite what's seen on TV police dramas, DNA is rarely featured in trials, which is when experts explain its reliability. "DNA evidence is seen to be so powerful, it's very difficult to defend yourself if you've got your DNA matched," says McCartney. If you're a law-abiding citizen with nothing to hide, you may still be asking yourself the question: where's the harm in using my DNA to help catch a killer? The answer depends on your personal ethics and how you weigh the benefits for victims against potential costs to other people.

THE SMALL PRINT

One key issue is informed consent. "I'm really not confident that people understand or are even aware that their genetic genealogy can be used for criminal or forensic purposes," says Dr Benjamin Berkman, a bioethicist at the US National Institutes of Health. Until recently, he adds, information about such disclosures was 'buried in the small print'.

Berkman says the problem stems from expectations. People signed up to GEDmatch to study their family history, not aid law enforcement. And although the site's original terms of service did warn users that DNA profiles could be used to help identify related victims or criminals, some members didn't realise that until DeAngelo's arrest hit the headlines, then felt so misled that they deleted their accounts. GEDmatch has since revised its terms to explicitly state that profiles could help identify a perpetrator of a violent crime.

Informed consent also means being conscious of the impact 'familial searching' could have on others. "I like to think about it in terms of your cousin getting arrested," explains Berkman. "Some would say 'The fact that my DNA indirectly helped to lead him to justice, it's fine', but you can imagine other people who would feel guilt or conflict about having caused a relative to go to jail."

When someone is under suspicion for a crime, their name can get leaked to the press – and in contrast to the criminal justice system, in




Michael Usry Sr with a picture of his then 19-year-old son. Usry Jr was vilified online as a murderer due to partial DNA evidence, but was later found innocent

In contrast to the criminal justice system, in the media you're often guilty until proven innocent

the media you're often guilty until proven innocent. That's what happened to US filmmaker Michael Usry Jr, who was investigated in 2014 for a 1996 murder, based on a partial match to his father's DNA following a familial search of a database (the FBI even secured a warrant for cheek swabs). Even if you're later cleared, as Usry was, being branded a killer could still haunt you for the rest of your life.

"At the end of the day it's your genome," Berkman concludes. "And if you want to learn more about your ancestry or your genealogy or your health, I don't know that other people get to tell you what you can and can't do with your DNA."

But for genetic genealogist CeCe Moore, the ethical balance tips toward the victims of crime and their families. "These families have often been waiting for decades for justice and some sort of closure," she says. "And we are finally able to provide that through this new technology and techniques." 

Dr JV Chamary is a writer with a PhD in molecular evolution and genetics. He covers science and technology for *Forbes.com*.



Watch *Last Chance Lawyer NYC*
bbc.in/2yVY5oy

Neurozan[®]

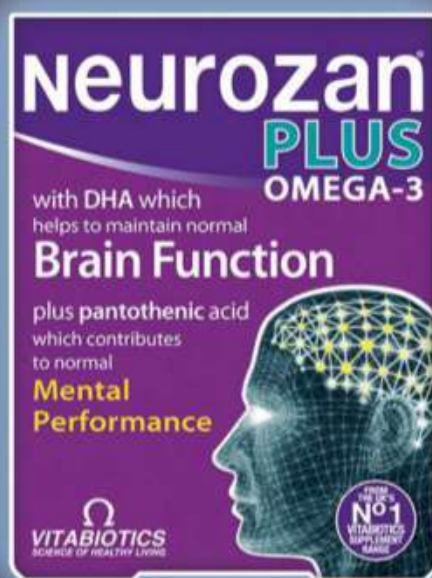
Feed your mind[™]

Neurozan[®] is a comprehensive supplement with over **25 nutrients** and amino acids to support your daily intake. Including **pantothenic acid** which contributes to normal **mental performance**.

Neurozan[®] Plus includes the original tablet, plus an Omega-3 capsule containing **DHA** which contributes to normal **brain function**[†].



Original
OVER 25 NUTRIENTS



Plus Omega-3
DUAL PACK

Britain's No.1 Vitamin Company*

*Nielsen GB ScanTrack Total Coverage Value Sales 52 w/e 16 June 2018.

From , Holland & Barrett, Tesco, Waitrose, independent pharmacies & health stores, www.neurozan.com

[†]A beneficial effect is obtained with a daily intake of 250mg DHA.



The **ONLY** vitamin company to twice receive **The Queen's Award For Innovation**



GENETIC MUGSHOTS

DNA found at crime scenes can also provide clues through ‘genetic phenotyping’ – where physical descriptions and photofit images are reverse engineered from recovered material. Parabon, the company that cracked ‘cold cases’ with genetic genealogy, says it can predict a suspect’s genetic ancestry and what they look like. Here are some cases they’ve worked on...

Troy and
Ladonna
French



TROY & LADONNA FRENCH *Reidsville, North Carolina*

Troy and LaDonna French were woken in the early hours of 4 February 2012 by the screams of their 19-year-old daughter Whitley. Rushing into her bedroom, they found an intruder holding her at knife point. The intruder released Whitley and fled downstairs, but as Whitley’s parents gave chase, he pulled out a handgun and fatally shot them both.

The intruder left traces of blood on the bannister. The police were able to produce a DNA profile from the blood, but it didn’t match any records on file or anyone known to visit the French household, including Whitley’s boyfriend John Alvarez. Subsequent testing, however, did indicate that the suspect might be related to John, but not through common paternal lineage, seemingly ruling out his father and brother, José Snr and José Jnr.

In 2015, Parabon performed DNA phenotyping on the DNA sample recovered from the crime scene. The result was a physical description and photofit that strongly resembled John Alvarez’s brother José Jnr. As a result, a DNA sample was collected from José Jnr that not only matched him to the crime scene, but also showed José Snr was not his biological father. José Alvarez Jnr pleaded guilty to double murder in 2016.

BRITTANI MARCELL

Albuquerque, New Mexico

Arriving home around midday on 11 September 2008, Diane Marcell found her 17-year-old daughter Brittani lying on the floor covered in blood. Standing nearby was a man holding a shovel, which he dropped before grabbing a knife and threatening Diane, who ran out of the house screaming for help.

Brittani survived the attack, but was left blind in her left eye, deaf in her left ear and suffering from memory loss.

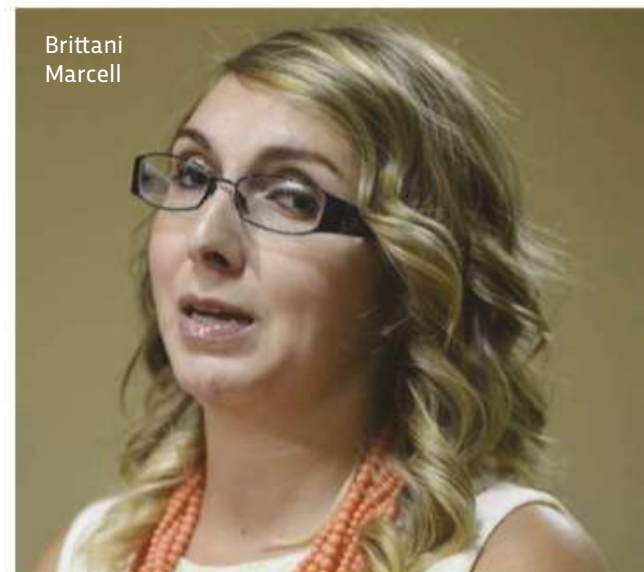
Police investigating the scene later found blood on the broken dining room window through which the man escaped. But DNA extracted from the blood failed to match any on record and, despite continuing efforts over the following years, the case hit a dead end.

Detective Jodi Gonterman, was assigned to the case in 2013, and continued to collect any information that Brittani was able to remember, which included a recollection of a boy called Justin Hansen who was a friend of her sister’s. In 2016, Gonterman submitted a sample of the blood found on the broken glass to Parabon for phenotyping. It suggested the suspect was of European

descent with some Native American lineage, and had brown hair, fair skin and green or hazel eyes – a description that bore a startling resemblance to Hansen.

Hansen refused to supply a DNA sample to police, but undercover detectives were able to obtain one from a discarded cup and successfully matched it to the blood found at the crime scene. Hansen was arrested in 2017 on charges of aggravated assault and battery, and sentenced to 18 years in jail in 2018.

Brittani
Marcell



Justin Hansen
at his trial



ADRIENNE 'SUNNY' SUDWEEKS

Costa Mesa, California

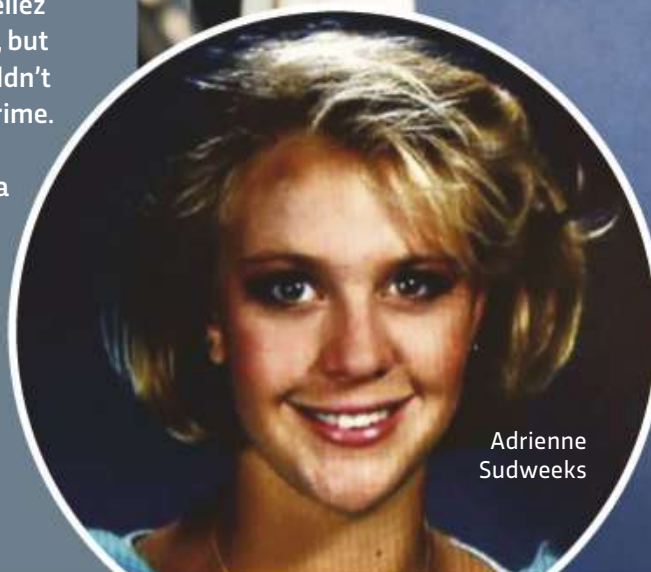
On 23 February 1997 Richard Johnson returned home from his night shift to find his girlfriend Adrienne 'Sunny' Sudweeks dead in the apartment they shared.

Detectives believed a man had raped and strangled her. The potential suspect's DNA was collected from Adrienne's body, but matched no records. The case went cold until April 2016 when the DNA sample was handed over to Parabon for phenotyping.

The process produced an image of a Hispanic male with brown eyes, dark hair and no freckles. It didn't fit any known suspects but later that same year Detective José Morales, who'd been assigned to the case, retested a fingerprint found on a door knob during the initial

investigation. That produced a match: Felipe Vianney Hernandez Tellez, who was arrested for spousal abuse in 2000, three years after Adrienne was murdered. The likeness produced by Parabon looked similar to a photo of Tellez the police had from his arrest, but without a DNA sample he couldn't be definitively linked to the crime.

In the intervening years, Tellez had fled to Mexico. But a DNA sample was collected from his son, who remained in the US, and indicated the suspect was a close relative. In early 2017, US authorities announced they'd seek Tellez's extradition so he could stand trial for murder, rape and burglary.



Adrienne Sudweeks

FELIPE HERNANDEZ-TELLEZ

PHOTO 2013-2016



SHAQUANA MARIE CALDWELL

Glen Burnie, Maryland

Anne Arundel County Police were called to the Glen Burnie area of Maryland on 14 June 2017 where they found decomposed human remains under a tarpaulin. Medical examiners were unable to identify the remains, but determined that they belonged to a female around 20 years old and that foul play was involved in her death.

The police contacted Parabon in late 2017 to see if the company could generate a likeness of the victim to assist with identification. Its phenotyping process was combined



LEFT: Shaquana Caldwell. RIGHT: Facial reconstruction of Shaquana created using genetic phenotyping.

with facial reconstruction using the victim's skull to produce an image of an African-American woman with brown eyes, black hair and no freckles that was circulated around the area where her remains were found.

Soon after the image was released, Baltimore City Police contacted investigators to say the image bore similarities to 26-year-old Shaquana Caldwell, who had been reported missing on 14 May 2017. Dental records confirmed the remains were those of Shaquana. Further investigation led to the arrest of her (unrelated) boyfriend Taras Caldwell, who later confessed to her murder.



LEFT: Ryan Derek Riggs. RIGHT: Facial reconstruction of Riggs created using genetic phenotyping

RHONA 'CHANTAY' BLANKINSHIP, *Brown County, Texas*

The body of Rhona Blankinship was found in an abandoned house 8km from her home at 5.20pm on Sunday 15 May 2016. She had been missing since Friday 13 May. Evidence suggested she was a victim of homicide and that a lawn mower blade, found nearby, was the murder weapon. An autopsy showed she had also been sexually assaulted.

A male DNA profile was produced from

recovered evidence, but it didn't match any on the police database.

Almost 18 months after the murder, the investigation had stalled and so a DNA profile was given to Parabon for phenotyping. It produced an image that suggested the perpetrator was likely to be a white male of European descent with brown/light-brown hair, blue/green eyes and some freckling. The description and image were released to the public.

Hours later, police were alerted to the image's resemblance to an acquaintance of Blankinship, Ryan Derek Riggs, who lived nearby. Riggs had gone missing by the time police arrived at his home, but reappeared about a week later at his local church where he confessed to the murder. He was arrested in November 2017 and is expected to stand trial in late 2019.



Rhona Blankinship



PSYCHOPATHS

THE PSYCHOPATHS AMONG US

Despite what Hollywood suggests, psychopaths aren't easy to recognise, since they're rarely seen brandishing blood-soaked axes while leering maniacally. So how can you spot a psychopath?

And could you be working alongside one right now?

WORDS: NICOLA DAVIES



Chillingly cool, collected and cunning. Is this the perfect description of a psychopath? Hollywood movies and popular culture generate such images of psychopathy. Be it Dr Hannibal Lecter in *The Silence Of The Lambs* or *Psycho*'s Norman Bates, such characters dominate the public's perception of a psychopath. But how close are these popular images to reality?

The term 'psychopath' originated in the 1800s, from the Greek words 'psykhe' and 'pathos', which mean 'sick mind' and 'suffering soul', respectively. However, this can be misleading. "Psychopaths might be better conceptualised as people who are dissociated," says criminologist

Robert Blakey. "In other words, people who are detached from their own emotions and the emotions of other people. Consequently, they just don't feel much. If they see a person in distress, psychopaths don't feel the distress themselves, so they have less emotional incentive not to harm people."

Blakey believes this dissociation can arise from inheriting an over-sensitive perceptual system. "If you're very sensitive to visible signs of distress and anger in other people, then seeing those signs could become overwhelming for highly sensitive children," he says. "A deficit in one's ability to predict other people's behaviour as a child can be a traumatic ➔

experience and, in response, the child's brain may dissociate." In other words, the empathy system shuts down to survive the emotions of others. The irony here is that people born with an excessive capacity to empathise could be more likely to develop psychopathic traits due to losing their full capacity for empathy in their efforts at self-preservation.

This has parallels with a theory about autism which, like psychopathy, is a disorder of social cognition. While autism is typically considered a deficit in cognitive empathy, or perspective taking, psychopathy is a deficit in emotional empathy. While the relationship between autism and psychopathy has gained increasing interest due to the shared lack of empathy, research indicates many distinctions between the two conditions. The most relevant distinction is that individuals with autism are not amoral, unlike psychopaths.

BORN TO BE VILE?

One way to identify a psychopath is to study patterns in their relationships. Psychopaths generally cannot sustain long-term relationships,

so short periods of intensity followed by detachment tend to define their close interactions. While in a relationship, their behaviour is likely to be highly manipulative and selfish, with their needs always coming first.

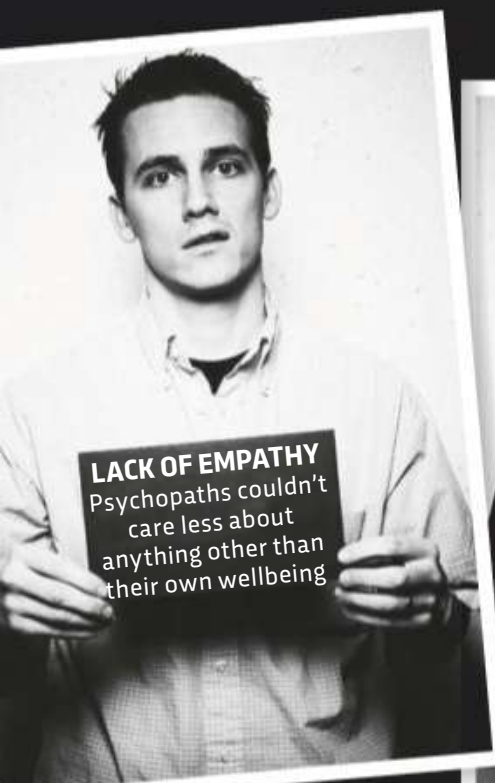
Not all psychopaths are violent criminals, but most present a threat to our welfare at some level – to one's peace of mind, sexual health or financial wellbeing. There are many theories for why psychopaths are the way they are. Some believe it is nature, or genetics, that causes psychopathy. Others think it is related to environmental factors. Whatever the cause, medically speaking, people with psychopathic tendencies demonstrate certain traits.

Researchers from Harvard University investigating decision-making in psychopaths took magnetic resonance imaging (MRI) brain scans of 50 prison inmates, with the intention of investigating the choices that psychopaths make. They found that people with signs of psychopathy had brains that were wired so that they over-valued immediate or short-term rewards. This desire for instant gratification overshadowed any concern about the consequences of their actions.

A psychopath's behaviour is likely to be highly manipulative and selfish

HOW TO SPOT A PSYCHOPATH

Here are some signs to look out for...



They also found that people who scored highly for psychopathy – as assessed by a delayed gratification test and the Psychopathy Checklist (PCL-R) – showed greater activity in the brain's ventral striatum. This is a key part of the reward system. In another study of 164 chimpanzees carried out at the University of Georgia, researchers found that a neuropeptide called vasopressin is associated with the development of socioemotional behaviours related to psychopathic personalities. This adds further support to a genetic element in the development of psychopathic traits. Environmentally, the impact of socialisation in a child's early years is perhaps equally influential in the formation of psychopathic behaviour. And according to Claudio Vieira, a clinical psychologist based at King's College, London, many personality disorders – including psychopathic personalities – may result from a combination of genetic elements that shape our personalities, life experiences and socioeconomic circumstances.

Psychopathic characteristics also vary by culture. A US and Netherlands study comprising over 7,000 criminals exhibiting psychopathic traits revealed that US-based offenders tended to

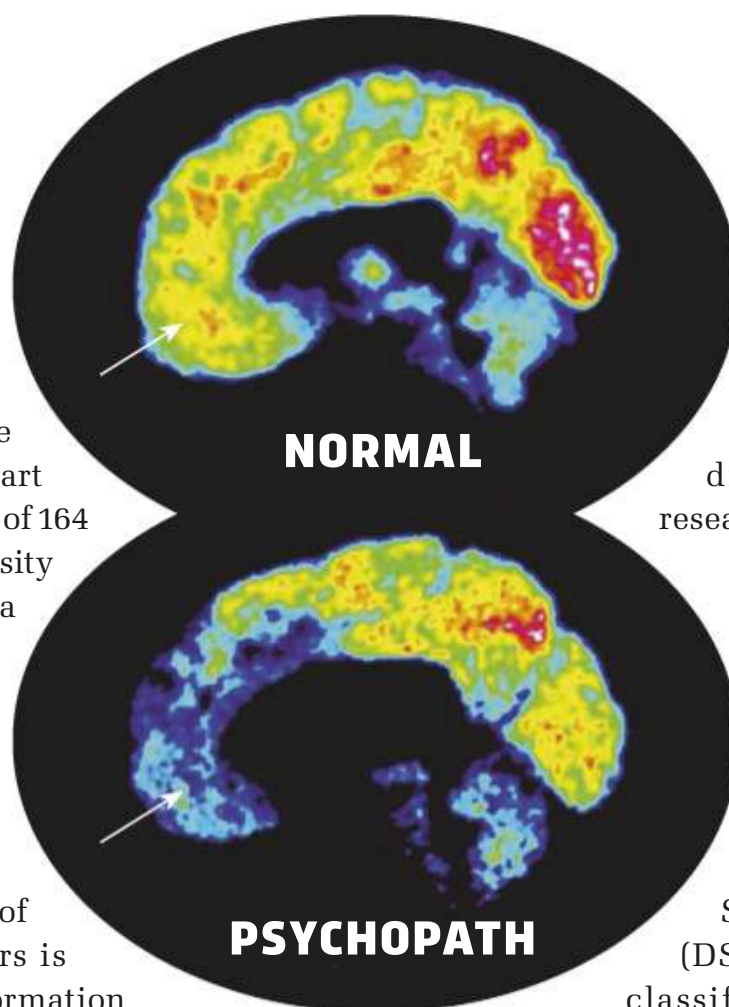
display callousness, while the Dutch offenders showed greater evidence of irresponsibility. These traits were measured using the PCL-R, which might be interpreted differently in different cultures. Nevertheless, the research raises some interesting questions.

A TOUGH CALL TO MAKE

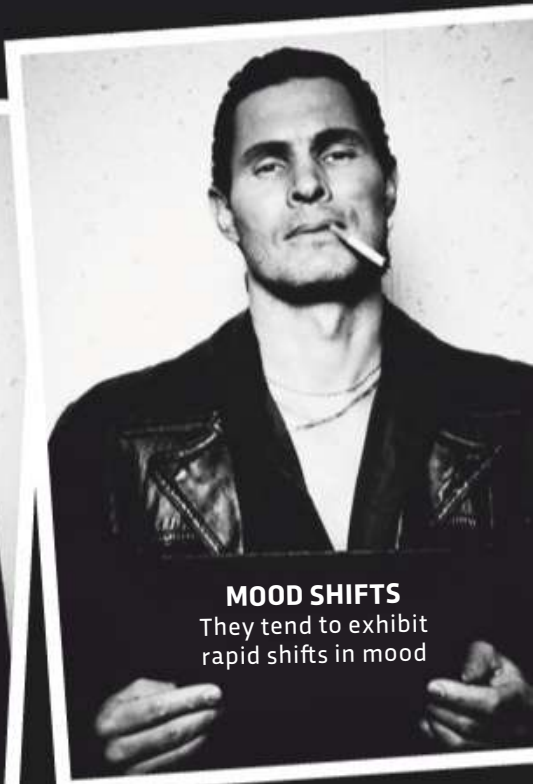
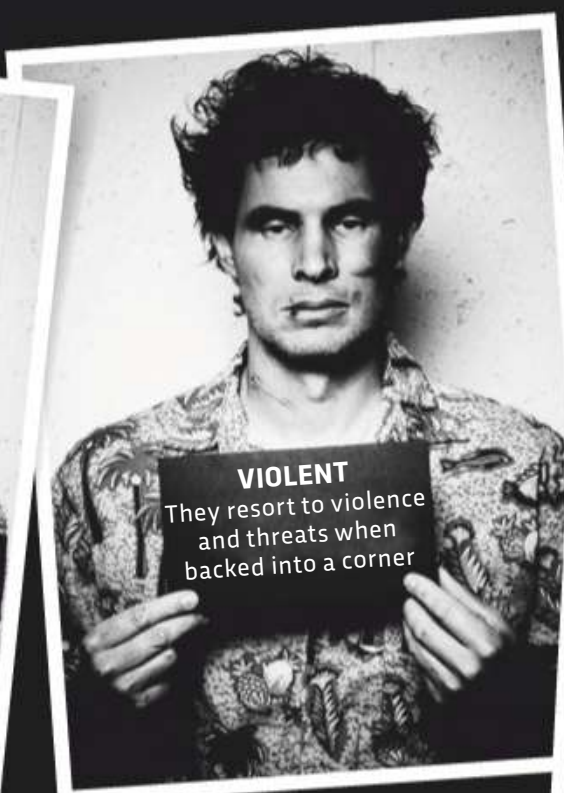
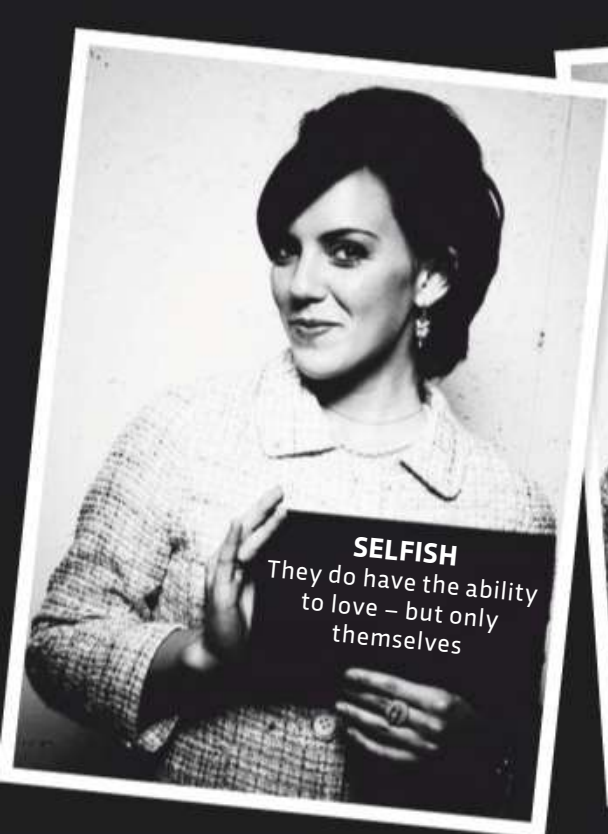
Be it nature or nurture, the popular image of a psychopath is influenced by the ambiguity surrounding its definition and diagnosis. Ironically, psychopathy is not actually an official diagnosis. In the Diagnostic And Statistical Manual Of Mental Disorders (DSM-5) – the official criteria used to classify mental disorders in the US – the closest condition to psychopathy is Antisocial Personality Disorder (APD).

“APD is characterised by impairments in personality functioning and by the presence of pathological personality traits. However, while offenders with psychopathy often have APD, offenders with APD are not necessarily psychopaths,” explains Vieira.

The closest thing to a checklist for identifying a psychopath is the previously mentioned PCL-R. This comprises a list of 20 character traits ➔



ABOVE: In the scan of the normal brain, there is activity in the frontal lobe (marked with an arrow), which is associated with emotional response; in the psychopath brain, there is little activity in this region



CAN PSYCHOPATHS BE TREATED?

There's no 'cure', but research suggests psychopathy can be made more manageable... if it's caught early enough

The traditional consensus among psychiatrists and psychologists has been that psychopathy is an untreatable condition. Even respected mental health professionals have bandied around terms like 'just evil' to describe psychopathic criminals. But while there's certainly no sign of a cure on the horizon, in recent years some evidence has emerged to suggest that young psychopaths, in particular, can at least be taught to manage their condition.

In 2001, a study carried out by Michael Caldwell and Gregory Van Rybroek at the Mendota Juvenile Treatment Center in Wisconsin in the US, found that young offenders diagnosed with psychopathic traits were far less likely to re-offend if given 'decompression therapy'. This involves moving slowly from a punitive model of care to one of positive reinforcement, in which youths were rewarded for more 'normal' behaviour. Since then, this treatment is said to have reduced rates of re-offending by a third.

More recently in 2012, David Bernstein, a professor of forensic psychotherapy at the University of Maastricht, began using an approach that he calls 'schema therapy', which focuses on encouraging patients to re-access the emotional and empathetic responses he believes have often, in psychopaths, become 'locked away' due to trauma or abuse during childhood. It's still early days for a treatment of this kind, but the initial results are promising, suggesting that offenders with psychopathic tendencies are less likely to re-offend if they've undergone schema therapy. And unlike decompression therapy, schema therapy seems to work for adults as well as for young offenders.



ABOVE: Broadmoor Hospital is a high-security psychiatric hospital that has housed a number of notorious patients, including Peter Sutcliffe, Ronnie Kray and Charles Bronson

ABOVE RIGHT: Some mental health professionals have claimed that Donald Trump could be a psychopath

and behaviours – such as a lack of remorse, failure to accept responsibility and emotional shallowness – to help determine if an individual is on the psychopathy spectrum.

The checklist isn't a clear-cut formula for diagnosis, however, as psychopathic traits can be hidden or subtle. And the chances are you know people who display some of them – because the majority of people have psychopathic tendencies. In most people they may be situation-specific or low level, but psychopathic traits aren't restricted to 'full-blown' psychopaths. "Most people with psychopathic traits blend beautifully into the fabric of our everyday lives," explains Dr Paul Hokemeyer, a clinical and consulting psychotherapist based in New York.

MURDEROUS MINORITY

The lack of a diagnostic tool or a presence in the DSM-5, is partly due to the mystery surrounding psychopathic behaviour. This has led to the predominantly inaccurate media image of a psychopath.

"The nature of cinematic and literary depictions is that they overdramatise the traits found among psychopaths by having them brutally murder a slew of victims," says Hokemeyer. "Top of this list include Javier Bardem's character in *No Country For Old Men* and Christian Bale in *American Psycho*. In real life, however, psychopaths seldom murder outright."

Prof Samuel Leistedt and Dr Paul Linkowski, forensic psychiatrists based in



Psychopathic traits can be subtle and chances are you know people that display them

Brussels, investigated the history of the cinema-psychopathy relationship in 2014 by analysing 400 films and shortlisting 126 fictional psychopathic characters on the scales of realism and clinical accuracy. They found that psychopaths were often caricatured as sexually depraved and emotionally unstable, with sadistic personalities and eccentric characteristics. Such images aren't necessarily realistic; indeed, Leistedt and Linkowski believe that certain cinematic psychopaths such as Norman Bates in *Psycho* and Travis Bickle in *Taxi Driver* are psychotics rather than psychopaths.


While psychopathy is a personality disorder underlined by callousness, recklessness, impulsive behaviour, lying and lack of empathy, psychosis refers to a mental state where the person has lost touch with reality. Psychopathy is typically not associated with any loss in the sense of reality: individuals know where they are and what they are doing. The perception that 'psychotic' and 'psychopathic' are one and the same simply isn't the case. While the former is an outward display of a chaotic

personality, the latter is more internal and difficult to spot. Far from being the crazed, damaged individuals portrayed in the movies, there is mounting evidence that many people with psychopathic characteristics are highly successful. "Psychopaths are very good at seeing which behaviours a system rewards and exhibiting those behaviours. This is one route to career success," says Blakey.

It's not surprising, then, that a 2016 Australian study found that around one in five US corporate leaders displayed psychopathic traits. Psychopaths may be poor at managerial tasks, but they are often adept at climbing the ladder by hiding weaknesses and charming their colleagues. Another potential benefit, according to Blakey, is that the typical psychopath doesn't care about other people's feelings and therefore they don't feel the same compulsion to protect them from negative emotions. As such, psychopaths find it easy to embark on emotional risks that other people might hesitate to take.

So while at extreme levels psychopathy can lead to antisocial and destructive behaviours, at moderate levels it can offer some advantages. The key difference is between 'clinical' and 'functional' psychopaths. Functional psychopaths know in which context to exhibit their characteristics. When it comes to goals, psychopaths have laser focus, persistent ambition, self-confidence and social charm. According to Hokemeyer, this functional aspect of psychopathy could be the real risk to society.

"The most dangerous trait of psychopaths is their ability to operate in stealth. On the surface, they can appear to be warm, genuine and incredibly charismatic," he says. "But just below the surface of their veneer lies a mountain lion waiting to pounce."

Beyond the Hannibal Lecters of the cinema, the story of the psychopath remains something of an enigma. Scientists know more about psychopathy today, based on case studies and brain research. Yet there is still much we don't know and the knowledge we do have is unsettling to many: psychopaths are not necessarily evil but regular human beings with a 'twist' – traits that make them adept at getting their own way. And they're living and working among us. 

Dr Nicola Davies is a medical writer and consultant health psychologist.

Is your boss a PSYCHOPATH?

According to an Australian study from 2016, one in five US corporate leaders displays psychopathic traits. “Psychopaths are very good at seeing which behaviours a system rewards and exhibiting those behaviours. This is one route to career success,” says criminologist Robert Blakey. Does that sound familiar at all? Have you been dropped in it by your boss or found yourself wondering how they managed to crawl their way up the corporate ladder? If so, this questionnaire might provide you with some clues.

Read the following 10 statements and rate how accurately each of them describes your boss.

- 0 = not at all
- 1 = sometimes
- 2 = definitely does apply

At the end, add up the ratings and see how they score.

Does your boss have any of these traits?

1 GLIB, SUPERFICIAL CHARM
Smooth, engaging, charming, slick and verbose – your boss is never shy, self-conscious or afraid to say anything. She’s never tongue-tied and doesn’t seem to be bothered about social conventions, such as taking turns talking.

0 1 2

2 GRANDIOSE SELF-WORTH
As far as your boss is concerned, he’s absolutely convinced that he’s the best employee to ever set foot in your building. He’s opinionated, cocky and loves to brag. Psychopaths are arrogant, and generally believe they are superior to the rest of the human race.

0 1 2

3 PRONE TO BOREDOM
Does your boss delegate every boring job she’s given to you? Psychopaths often have low self-discipline when it comes to dull or routine tasks. They fail to work at the same job for any serious length of time.

0 1 2

4 PATHOLOGICAL LYING
Deceptive, sly and manipulative, your boss seems to have an answer for everything, only you’re not sure if those answers are true.

0 1 2

5 LACK OF REMORSE OR GUILT
Cold-blooded and remorseless – psychopaths never seem affected by the misfortune of others. NB: a lack of sympathy for the ‘headache’ on Monday morning that stopped you coming into work doesn’t count.

0 1 2

6 SHALLOW AFFECT
They seem to have a limited range of emotions. Although she’s friendly on the surface, you actually have a very shallow relationship with your boss. Do you ever wonder why she never seems that bothered about your life outside of the office?

0 1 2

7 CALLOUSNESS AND LACK OF EMPATHY
Behind other employees’ backs your boss shows little empathy. He can be so cold and inconsiderate that sometimes he makes the Terminator look like a teletubby.

0 1 2

8 PARASITIC LIFESTYLE
Your boss only helps when it benefits her to do so. Psychopaths avoid responsibilities and will often exploit others for their own gain. Does she only offer to make a cuppa when there’s a task she needs your help with?

0 1 2

9 POOR BEHAVIOURAL CONTROLS

Is your boss irritable, quick to anger and impatient? Does he follow this up with threats, aggression and even verbal abuse? Psychopaths struggle to control their anger, often acting hastily only to apologise later, in the hope that you'll maintain a good impression of them.

0 1 2

10 IMPULSIVITY

Being impulsive can be a good thing, but not if it means your boss takes half the day off to go sky-diving, leaving you with all the paperwork. Does she seem to find it hard to resist temptation and frustration?

0 1 2

SCORE

0–5

Breathe easy, the office kettle poses more danger.

6–10

Don't worry, you're safe... probably.

11–15

Hide the staplers and any sharp objects.

16–20

Results from this test cannot be used in a court of law.

DISCLAIMER

This test is loosely based on the Hare Psychopathy Checklist, the test used to identify psychopaths. Please note that Dr Hare does not recommend that laymen attempt to 'diagnose' friends and family, and suggests that only qualified psychologists with hundreds of hours of training can accurately and appropriately apply the checklist. That said, this list is intended to give you an understanding of the traits psychologists look for when attempting to identify a psychopath.



Jon Ronson

The author of *So You've Been Publicly Shamed* discusses his journey into madness and the psychopaths he met while researching his 2012 book *The Psychopath Test*

Why psychopaths? What compelled you to meet and write about these people?

Years ago I made this film about a man called David Icke. He believes that giant, blood-drinking, paedophile lizards rule the world and everybody thinks he's nuts. But then, you've got all these eminent psychologists who basically believe the same thing – that there are people with lizard-like qualities that are in charge.

They're referring to the psychopaths at the top of the [corporate] tree. That gave me the thought that madness might be a more powerful engine than rationality when it comes to how the world turns. Basically, calm, happy, rational people just tootle on with their lives, not creating any waves. The people who would be classed as disordered are the ones that actually run the world.

Now, I always kind of worked around the possibility that some of my interviewees might actually be mad. It became a bit like the elephant in the room, so eventually I had to confront this possibility. Then I very quickly got into the questions like 'What is mad?' 'Who decides what is mad and what does that mean?'

So how did your views on psychopaths change as you worked on the book?

I always go into my stories with no real preconceptions because I just want to go where the story takes me. But I was most struck when I met one of the guys on the Fortune 500 [the annual list published by *Fortune* magazine of the top 500 companies in the US] to see whether he showed any similar traits to the psychopathic patients I had met. It was amazing. I was totally shoe-horning him into what I had been taught about psychopathy. Whenever he did something that was sort of reasonable I was really disappointed and I tried to shove it under the carpet.

It was then that I realised being a qualified psychopath spotter could turn me psychopathic – it dehumanised me. Writing this book taught me just how close we are to dehumanising others and consequently dehumanising ourselves.

What was it like to meet a psychopath?

Quite often there is a sort of superficial charm. There was this guy in the book – Tony from Broadmoor – who was just a nice, charming, young man. But then his psychiatrists would say, you've got to be very careful [around him]. But that's quite alarming because there's nothing whatsoever about his demeanour that would suggest you've got to be careful. He's just somebody you'd like to hang out with.

But when I met Emmanuel 'Toto' Constant, the Haitian death-squad leader, I really got the sense that this man is like an unexploded bomb. So it does vary.

Did you feel duped by Tony's charm then?

I was aware of his crime, but it was a long, long time ago. Tony has this fascinating story. He says he faked madness, to get a softer sentence. But in the end they sent him to Broadmoor. Basically, if he hadn't faked madness and just gone to prison, he'd have been out years ago because prisons are full of psychopaths, they're just not in the mental health system. But because the psychologists at Broadmoor believe he's a future danger to himself and others, he hasn't been let out.

At first, the obvious thing to think about Tony is either he's suffered a miscarriage of justice or he's a psychopath. It took me quite a long time to realise he's both. Just because he's a psychopath doesn't mean we can't have positive feelings about him.

What about yourself – did you find yourself wondering whether you had any psychopathic traits?

I'm the antithesis of a psychopath – I'm full of anxiety. I feel like there's somebody living inside of my face just lighting up matches on my skin. That's the opposite of psychopaths – they tend not to feel anxiety.

But then I started psychopath spotting and suddenly I turned into one. In general, you couldn't meet a less psychopathic person than me. I wish I was a bit more psychopathic sometimes, because I wouldn't have such a mass of anxiety.



A composite image of a man's profile, facing right. Inside his head, a detailed cityscape is visible, with skyscrapers and buildings. The image has a warm, golden-brown color palette.

CATCHING CROOKS

How the advent of psychological profiling revolutionised police investigations, helping to catch some of the world's most notorious criminals

WORDS: ANDY RIDGWAY

A crime scene is a window into a criminal's mind, allowing detectives to gain insights into what makes them tick and how they behave that can be used to lead them to the culprit. Or at least that's what we're lead to believe when we watch films like *Silence of the Lambs* or TV series like *Cracker* that feature psychological profiling. But how true is this? Can a crime scene really be picked apart and used to probe the inner workings of the criminal brain?

While attempts to psychologically profile criminals date back centuries, the first well-publicised case that involved profiling is that of the 'Mad Bomber' who planted over 32 home-made bombs in some of New York's most crowded spaces, such as theatres, a subway station and a library during the 1940s and '50s. After 16 years of unsuccessfully trying to catch the bomber, the city's police force turned to James A Brussel, a private psychiatrist.

Brussel pieced together a profile of the bomber from letters he wrote threatening further attacks as well ➔

as crime scene photographs. Brussel called his technique ‘reverse psychology’. The letters, sent to newspaper editors, were written in nearly perfect block letters. This demonstrated, said Brussel, that the bomber was “almost certainly a very neat, proper man”. As well as predicting that the culprit would be a paranoid schizophrenic, in his mid-40s, Brussel most famously told the police that when they caught the man responsible for the attacks, he would be wearing a double-breasted suit. “And it will be buttoned,” he said.

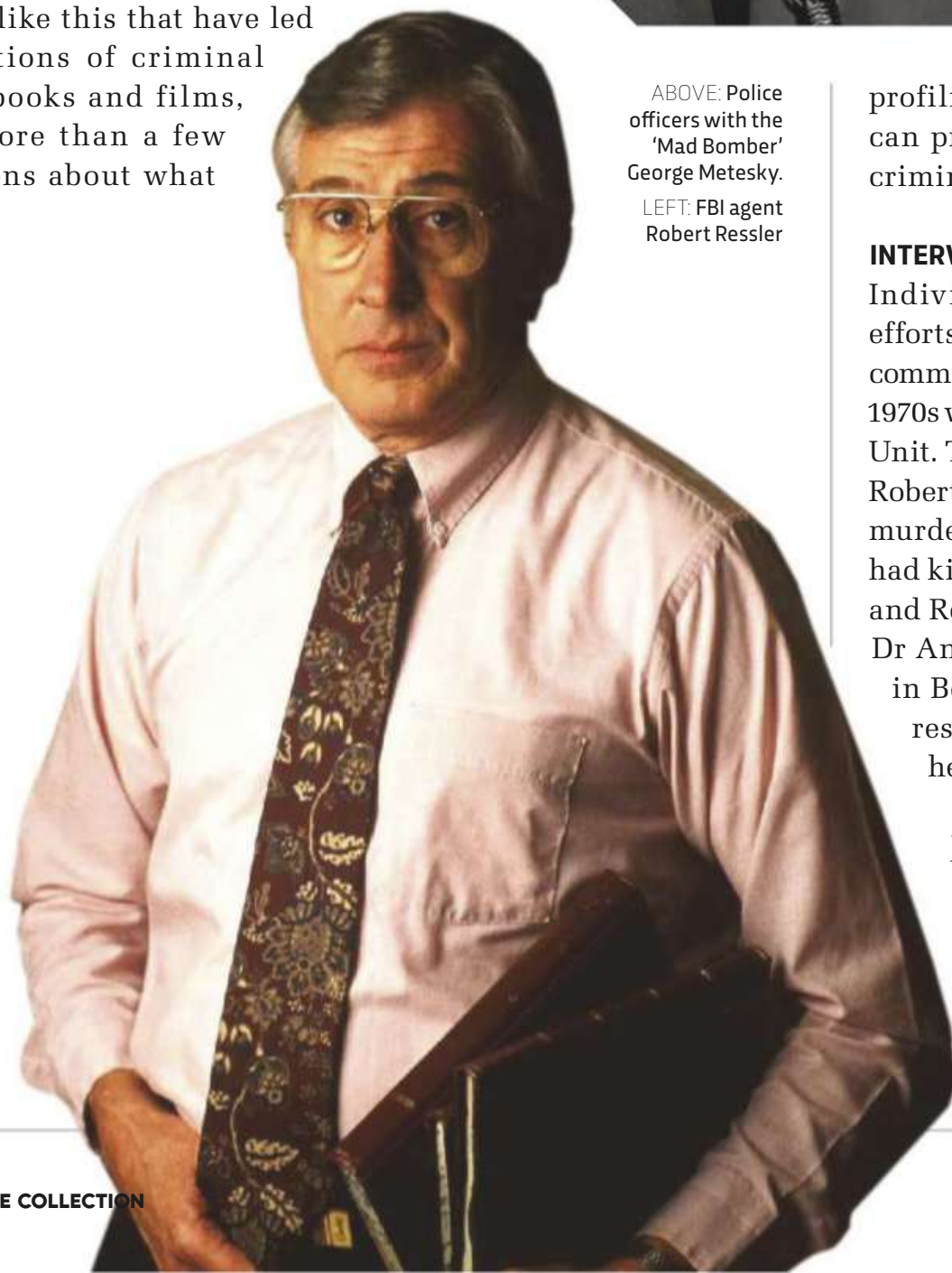
When the police entered the home of George Metesky, the man behind the bombings – having tracked him down with the help of the profile – he was wearing burgundy pyjamas. When asked to get dressed, he emerged from his bedroom wearing a brown sweater and, somewhat eerily, a double-breasted blue suit.

It is stories like this that have led to the depictions of criminal profiling in books and films, as well as more than a few misconceptions about what



ABOVE: Police officers with the ‘Mad Bomber’ George Metesky.

LEFT: FBI agent Robert Ressler



profiling can achieve. That said, psychology can provide some powerful insights during criminal investigations.

INTERVIEWING MURDERERS

Individual cases aside, the first concerted efforts to climb inside the minds of criminals committing the most heinous crimes came in the 1970s when the FBI set up its Behavioural Science Unit. Two agents of the day, John Douglass and Robert Ressler, set about interviewing 36 serial murderers in US prisons who, between them, had killed no fewer than 118 people. Douglass and Ressler were assisted in their research by Dr Ann Wolbert Burgess, a psychiatric nurse in Boston who had also conducted her own research into rape victims and was using her findings to teach trainee FBI agents.

“I was listening to what Bob Ressler and John Douglass were doing when they were in prisons talking with convicted offenders,” says Burgess, who is now a Professor at Boston College Connell School of Nursing. “They were not collecting systematic data, so our first task was to come up with a data



sheet and it came to 57 pages.” This data sheet outlined all the information FBI agents should collect for *all* of the serial murderers, including evidence collected at crime scenes, the criminal’s background and how they were eventually caught. The idea was to apply techniques from scientific research, being methodical and consistent in how data was collected, to these prison interviews. By doing this it would allow different cases to be compared and patterns to be found.

It’s an era in the FBI’s history captured in the Netflix series *Mindhunters*. Burgess is represented as Dr Wendy Carr in the series. While some aspects of Burgess’s background have been changed – Carr for instance is a psychologist rather than a psychiatric nurse – the series shows the influence Burgess had on these early days of profiling.

The insights from interviews with the 36 murderers enabled the FBI to make inferences in live criminal cases. “Because we had this 36 as a base to delve into, they would say maybe he was in this age range, in this type of work, or maybe he lived in this particular area,” says Burgess. “So the police would take ➔

CAN PROFILING BE USED TO CATCH TERRORISTS?

Terrorist acts are typically well planned, making the task of developing profiles from the scant evidence left behind difficult. The case of the ‘Mad Bomber’, who planted over 32 home-made bombs in some of New York’s most crowded spaces, shows that profiling can be successful.

But then there’s the case of the Unabomber, Theodore Kaczynski, who carried out 16 attacks in the US between 1978 and 1995 which left three people dead. When he was arrested in April 1996, Kaczynski matched seven of the 12 items on a profile the FBI had published the year before. However, the most significant factor behind his arrest was his brother recognising phrases and ideas in a manifesto he wrote and that was published in national newspapers.

The rise in the number of terrorist incidents in recent years has led to a rise in profiling research, with studies focusing on how individuals become radicalised and what leads them to commit violent acts. Detained terrorists have been interviewed to see if there are any tell-tale psychological characteristics. In one study, published in *Nature Human Behaviour* in 2017, interviews with incarcerated paramilitary terrorists in Colombia showed their moral compasses to be skewed. Acts of intended harm, such as attempting to poison someone, were viewed as being *more* acceptable than accidental harm. In other words, the ultimate goal behind the terrorist acts is seen to justify any deaths.

Turn to p76 to see how maths is providing new insights into terrorism.



Police officers bring Theodore Kaczynski to court

5 CASES CRACKED WITH CRIMINAL PROFILING



THE RAILWAY RAPIST

Police investigating a string of rapes and murders of women near railway stations across London from 1982 called on the services of Prof David Canter, then at the University of Surrey. Canter handed the police a detailed profile that resulted in them placing John Duffy, who was ultimately convicted, under surveillance. Canter used his consistency principle – that what offenders do when they commit a crime is an expression of how they behave the rest of the time – to develop the profile.



THE BOSTON STRANGLER

One of the distinctive aspects of the crime scenes left behind by the Boston strangler was the serene facial expressions of his victims. James Brussel,

the psychiatrist who had made a name for himself by helping to catch the Mad Bomber, felt that this showed his victims knew their killer – he may have befriended them beforehand. Brussel's profile, which helped the police catch Albert DeSalvo, also described him as being neat and tidy – no fingerprints were left at the crime scene – and athletically built, his victims having apparently passed out instantaneously from strangulation.

THE NOTORIOUS SERIAL KILLER

Charming and charismatic, Ted Bundy is one of America's most notorious serial killers. While the man who confessed to killing 30 young women and girls in seven

states in the 1970s was not caught using profiling, his was a profile that ensured he was kept behind bars. He was first imprisoned in 1975 for the aggravated kidnapping of a young woman in Utah. Among the team of psychiatrists called in to write a report on Bundy was Dr Al Carlisle, who determined he was a highly violent person who was likely to continue to kill if set free.



THE VAMPIRE OF SACRAMENTO

Richard Trenton Chase earned his nickname by drinking the blood of his victims and eating their body parts. Bob Ressler at the FBI's Behavioural

Science Unit was called by Sacramento Police Department following the murder in January 1978 of a 22-year-old Teresa Wallin after which Chase is reported to have collected her blood in a yoghurt cup to drink. The Unit's profile included the fact that Chase would live within a mile or two of where a car used in the aftermath of a subsequent attack was abandoned. This and most of the other aspects of the profile turned out to be accurate.

THE BITER

In September 1983, the remains of a 13-year-old paperboy were found in a ditch in Nebraska. He had bite marks all over his body. The FBI were called in and a profile developed. Three months later, another Nebraska boy was murdered and he too had bite marks all over his body. When 19-year-old John Joubert came to the police's attention after being spotted loitering outside a daycare centre, he matched the FBI's profile and he was arrested, confessing to two murders. Joubert was subsequently convicted of these and a further child murder that had taken place in 1982.



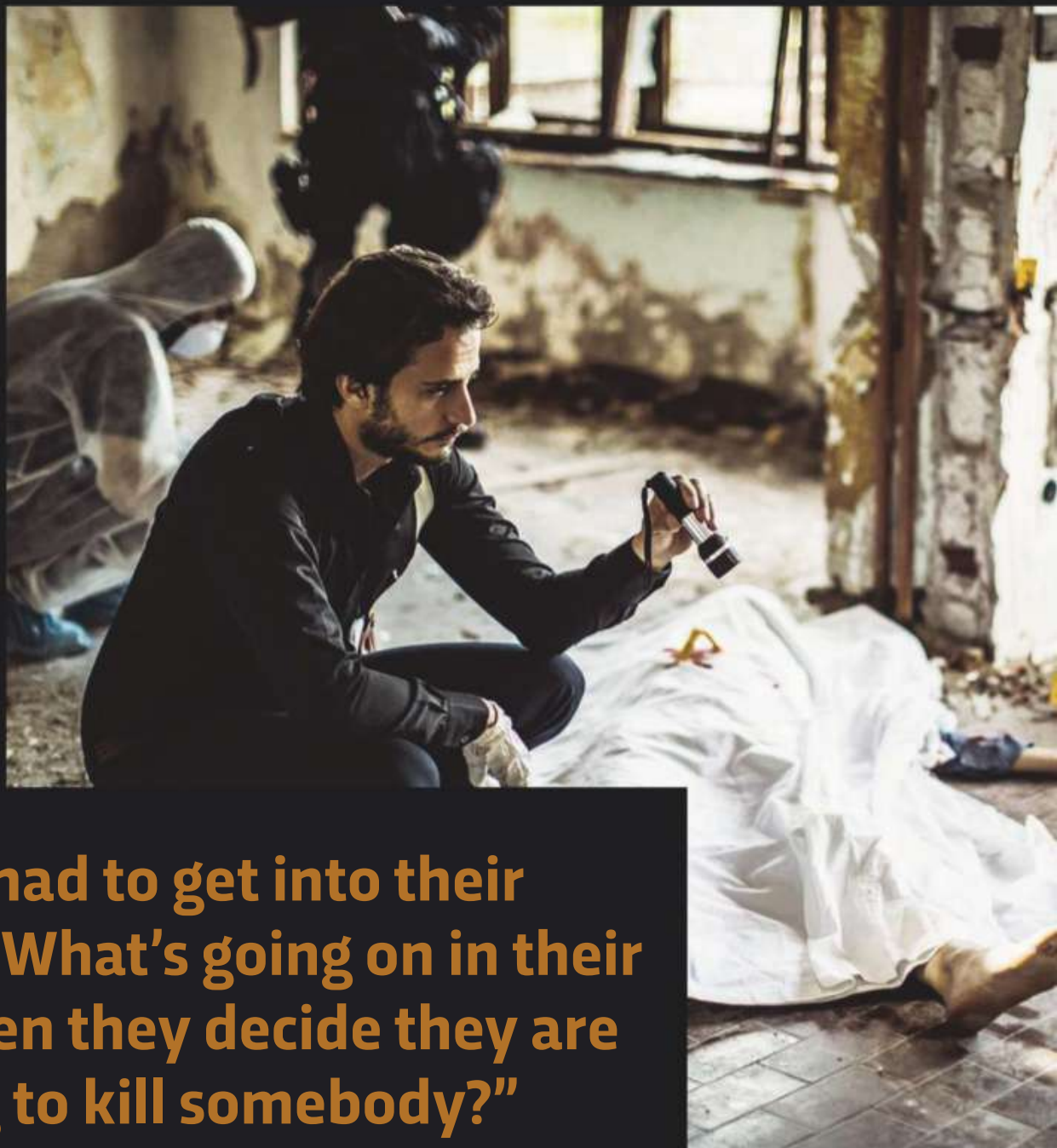
PRESS ASSOCIATION, GETTY X2

Evidence collected at a crime scene can help to build a criminal profile

that profile and go back to the suspects they had and say ‘oh my gosh it looks like this guy’ and they would go back and re-interview him.”

One of the central theories of the time was that serial killers could be split into two types – organised and disorganised. The crime scenes of organised murderers would show obvious signs of planning; restraints would often be used on the victim, the body hidden and the murder weapon would not be found by police officers. With disorganised murderers, the attack would be spontaneous; the victim would often be known to the murderer and the body left in view. As well as the crime scene differences, organised murderers were characterised as being intelligent, socially competent and would tend to follow the crime on the news media. The disorganised criminals were said to be of average intelligence, socially immature and would have little interest in how the murders were covered in the media.

“What we were able to determine just from our 36 serial murderers gave agents enough direction when they would get a case in from the field to be able to personalise it a bit – look for someone in his 20s, look for someone who lives within a one mile radius of the crime who may have recently lost their job,” says Burgess, who published numerous scientific papers and books based on her work with the FBI. “The other thing that was really important was the development of the fantasy of the serial murderer; what’s going on in their mind when they make the decision that they are going to kill somebody,” says Burgess, who still works as a consultant on criminal cases. “Thoughts



“You had to get into their thoughts. What’s going on in their mind when they decide they are going to kill somebody?”

drive behaviour, so you had to get into what were their thoughts.”

The FBI’s early profiling work has been influential. “The great strength that really got me moving was that they said the behaviour in a crime needed to be looked at closely because people had not really done that,” says Dr David Canter, an Emeritus Professor at the University of Liverpool. Since those earliest days, profiling has been used extensively – in the US at least. By the mid-1980s, the FBI was generating 300 profiles each year and by the early 2000s, this had grown to over 1,000 profiles a year. Canter, who is known for the help he gave British police in detecting the ‘railway rapist’ in the 1980s (see ‘5 Cases Cracked With Criminal Profiling’, opposite), is critical of some of the FBI’s approaches.

One of Canter’s criticisms is that criminals don’t neatly fit into two categories – organised ➔



and disorganised. In one of his studies, he and fellow researchers at the University of Liverpool analysed the details of 100 murders conducted by 100 serial killers and found that all contained aspects that were organised and, to a lesser extent, disorganised. “If you are going to get away with killing over and over again, you have got to be reasonably organised,” says Canter. Even the FBI later recognised a ‘mixed’ category of serial killer.

Other criticisms have been levelled at the FBI’s profiling techniques too. Despite Burgess’s efforts to add scientific rigour to the techniques, some FBI profiling has been criticised for being overly reliant on the experiences of previous cases by profilers, who also allow their intuition to help shape profiles, rather than purely making insights based on cold, hard scientific evidence.

Canter has moved in his own direction, developing the field of investigative psychology. The idea being that psychology can help in criminal cases in a much broader way than by providing profiles of culprits, also helping with aspects, such as interviews with suspects, as well as when and where to use surveillance

Arson attacks can be split into those aimed at a person and those where the focus is the object itself being burnt

techniques. The field also uses scientific research techniques.

“It’s all probabilistic,” says Canter. “That’s the important point to be clear about. It’s not like Sherlock Holmes who definitely, supposedly, tells you about the suspect. It’s the probability the individual will attack at the weekend, in this sort of area, that the individual is probably known to the police for burglary. These sorts of areas that help to shape police activity.”

One of Canter’s studies looked at 175 solved arson cases from across England. Crime reports and witness statements from the arson attacks revealed that arsons can be split into those aimed at a person and those where the focus is the object itself being burnt. They can also be divided into those that are expressive (the need to express anger or other emotions) and those that are instrumental (where the motivation is more functional, such as to destroy a car used in a robbery). Each of these categories of arson reveals itself in a different way at the crime scene. In an expressive arson attack directed at an object for example, the target may have some emotional significance – it could be a public building or hospital for example.

“It’s all probabilistic. It’s not like with Sherlock Holmes who definitely tells you about the suspect”

In such cases, the arsonist is likely to have a history of setting fires and will often hang about at the scene of the fire.

Characterisations such as this have been developed by Canter and his colleagues over the past 25 years not just for arson, but also other crimes such as rape, burglary and murder.


“What I talk about when I talk to police officers about this is identifying what is salient about a crime,” says Canter. It’s these key factors that reveal something about the motivation behind a crime.

COMMON TRAITS

Many other psychologists have also been trying to gaze into the minds and lives of criminals, searching for patterns. While there’s isn’t anything that could be regarded as a typical serial killer profile – as many are quite different from one another – it’s thrown up some interesting results. For example, the likes of Fred West from Gloucestershire, who committed at least

12 murders, and American hitman Richard Kuklinski, grew up in households in which they were abused or neglected, and brutality was normalised. Other research has shown that serial killers tend to work in some jobs more than others, such as truck driving.

Despite his successes, Canter is frustrated that British police forces have not embraced ideas from investigative psychology to a greater extent. “It’s not as if I’m some sort of crank working in a garage; there are hundreds of people who have studied with me, including lots of police officers,” says Canter. He says his attempts to work with police forces have been thwarted, as police staff he has been working with have moved on, as well as a focus by the police on solving current crimes rather than the long-term development of new investigative systems.

Frustrations aside, psychological profiling continues to be an active field of research, with certain areas, such as the profiling of terrorists (see ‘Can Profiling be Used to Catch Terrorists?’, on p43), expanding rapidly in recent years. But it will always have its limitations, something even the celebrated profiler James A Brussel, who helped catch the Mad Bomber, was aware of. In his book, *Casebook of a Crime Psychiatrist*, he wrote: “At times I was almost sorry I had been successful in describing George Metesky, for I had to live up to that success. It wasn’t always easy and it was sometimes impossible. But I continued to succeed often enough so that the police kept coming to me.” 

Andy Ridgway is a freelance science writer based in Bristol.

A forensic team mark out evidence at a bloody crime scene



THE TRUTH WILL OUT

FORMER CIA OFFICER PHILIP HOUSTON REVEALS HOW TO GET ANYONE TO TELL YOU THE TRUTH

WORDS: **JO CARLOWE**

Social psychologist Jerald Jellison famously claimed that humans are lied to 200 times a day. Little wonder, then, that reams have been written on how to spot a liar. But what do you do if you think someone has told you a fib? How do you convince them to tell you the truth when it may be in their best interest to lie? Well, former CIA officer Philip Houston, co-author of *Get The Truth*, believes he knows how.

In his 25-year career with the CIA, working as both an investigator and a polygraph examiner, he has eked confessions from some of the most entrenched liars, including terrorists and spies. And he says the techniques he uses in real-life counterterrorism and criminal investigations are applicable to all of us in our daily lives. There are methods that we can use in real-life situations to get a partner to admit to an infidelity, or a child to confess to a misdemeanour.

Surprisingly, the way to the truth has its roots not in relationship psychology, but in the science of persuasion. We obtain the truth by getting people to use short-term thinking. A shopping channel presenter, for example, will never say, “pick up your chequebook” because that will get viewers thinking about their finances (or lack of them). Instead, they will say, “pick up the phone”. Likewise, agents in pursuit of the truth will try to stop you thinking about the long-term consequences of your actions. And both salespeople and investigators use a ➔

GETTY





‘sales pitch’ to get you to switch focus away from your own goals and onto theirs.

SELL THE TRUTH

In the case of the criminal investigator, the ‘sales pitch’ is actually the interrogation. This differs from the initial interview, which is a dialogue in which the investigator asks questions and the suspect responds. By contrast, the interrogation is a monologue in which the investigator does most of the talking. It is akin to the marketer’s sales pitch, but instead of a product, the investigator is selling the idea that telling the truth is the only way forward.

“The interview is often not effective because each question is another opportunity to lie. With every lie the person tells, they become more psychologically entrenched [committed] in maintaining the lie,” Houston explains.

To overcome this, the interrogator can switch to a monologue to lead the person into short-term thinking, causing them to become temporarily more focused on the rationale provided in the monologue than the long-term consequences.

“If a person is truly thinking clearly and logically, they should never confess – confession is a losing proposition for them,” admits Houston. “When we are training law enforcement officers, we often joke that in the interrogation, they have to become an 8ft x 10ft [2.4m x 3m] condominium salesman. That is extremely difficult real estate to sell, but the concept of short-term thinking is so psychologically powerful that it makes their monologue effective and successful.”

The methods are universal and can be used to elicit the truth from anyone – not just hardened criminals. And it turns out that the truth is not so hard to reach, because humans actually like to unburden themselves. Indeed, a Canadian neuroimaging study from 2014 revealed that our cortical reward system is more active when telling the truth than when lying. In other words, we get more satisfaction from being honest.

“We tap the very same principle in every interrogation scenario we encounter, whether the aim is to get a terrorist to disclose the details of a bomb plot, a serial killer to confess to a murder or a child to admit they didn’t do their homework,” says Houston. The key to success



“The more you question someone who is lying, the more psychologically committed to their lie they become”

PHILIP HOUSTON, FORMER CIA OFFICER AND CO-AUTHOR OF GET THE TRUTH

WHAT MAKES SOMEONE MORE LIKELY TO LIE?

THEIR SOCIAL CLASS

US scientists have found that the upper classes lie more in negotiations and cheat to win money more than the lower classes.

When asked about values, the upper-class participants had more favourable attitudes towards greed, which may go some way to explain the correlation between social nobility and ethical ignobility.

THEY ARE PRESSURED FOR TIME

Psychologists asked participants to roll a die and to report the result to determine their pay.

Those given a short amount of time to report the outcome were more likely to lie. Experts suggest that when given more time, individuals are unable to inwardly justify lying and so they tell the truth.

THEY WERE RAISED BY LIARS

Children lied to by adults are also more likely to lie.

In one study, children were told there were sweets in another room. When the kids discovered there weren't any sweets, they were more likely to cheat and lie in a subsequent task than children who were not lied to at the outset.

IT'S THE AFTERNOON

We are more likely to lie in the afternoon than the morning. Studies show that we are 20 to 50 per cent more likely to be dishonest in the afternoon, by lying and cheating more in various tasks. Experts put this down to 'psychological depletion' – as the day wears on we become cognitively weaker.

THEY WANT PEOPLE TO LIKE THEM

Studies show that 60 per cent of people lie at least once during a short conversation with someone new and on average tell two to three lies. Women are more likely to lie to make the other person feel good, while men are more likely to lie to make themselves look better.

is to transfer to the monologue the moment you are confident that you are not being told what you need to know.

"Remember, the more you question someone who is lying, the more psychologically committed to their lie they become," warns Houston.

GOOD COP

So how do you switch from a friendly dialogue into the more serious monologue? Houston recommends you make what's known as a 'transition statement' that is a Direct Observation of Concern (DOC), an example being: "Something is clearly on your mind."

"The DOC is critical. It sends the simple message in a non-adversarial tone that everything the person has done to try to get away with the act of wrongdoing has failed. It psychologically orientates the person's thinking to the realisation that they need a new game plan, and the interrogator is perfectly positioned to provide that game plan via their monologue." In essence it says: 'You have failed so don't think your way anymore – think my way'.

In the 'interrogation phase' it is more effective to use statements rather than questions. "If you ask a question, it signals that you still don't know if they're guilty, so they still have a chance to convince you they're not," says Houston.

Statements suggest that the truth is a given. As more facts come into play, you can make your proclamations stronger. 'I know the who, I know the what, now I need to understand the why', is an especially useful statement.

"This particular approach is very effective because it causes the person to ask themselves 'why is the why so important?' The answer is often a realisation that the 'why' could influence the severity of the consequences," says Houston. "As a result, the person often initially fabricates or fudges on the 'why'. That's okay, because virtually any explanation of 'why' equals an admission of guilt. Once we have the confession, we can coax the real motivation out of them."

In a professional interrogation, the investigator may introduce a Direct Observation of Guilt (DOG) such as: "We can't eliminate you from our suspects." However, Houston only recommends the layperson uses the DOG if they have irrefutable evidence on which to base it.

When giving their monologue, CIA interrogators will minimise, rationalise and generalise the act of wrongdoing in order to bring the person closer to a confession. Statements like: 'We've all been there' or 'It's not the end of the world' are not unusual. A study from the University of Montreal's School of Criminology found that methods ➔



5 STEPS TO GET ANYONE TO TELL YOU THE TRUTH

1 KEEP THEM IN SHORT-TERM THINKING
You need the person not to dwell on the consequences of their actions, otherwise they'll worry about job loss, divorce etc. To achieve this, minimise the seriousness of the situation with statements such as: 'It's not the end of the world' or 'It's a fixable problem'.

2 SOCIALISE THE SITUATION
Make the person feel that there are others in the same boat, so they don't feel isolated. This can be done with a monologue that includes statements such as: 'It's nothing I haven't dealt with before' or 'In our world, this is the sort of thing that happens all the time'.

3 FOCUS THEM ON TELLING THE TRUTH RATHER THAN ON THE ACTION ITSELF
The person needs to be convinced that the only way out of their current predicament is to be completely truthful to you. Here is an example of a useful statement: 'This is a fixable problem. To fix it, we need to get everything onto the table. That's the only way'.

4 MAKE A DIRECT OBSERVATION OF CONCERN
Ask questions such as: 'Something is clearly on your mind' or 'Help me understand what I am missing'. With more facts, make the transition to a direct observation of guilt: 'I know the what and the who, but I need to know the why'. Or stronger still: 'Based on the facts, it is clear you did it'.

5 SLOW YOUR SPEECH, TALK SOFTLY AND BE POLITE
If you rant, the person will focus on your behaviour rather than their own and become resistant. Choose your words carefully. For example, 'you took' rather than 'you stole', otherwise you'll conjure fears of job loss or prison and the person will quickly become defensive.

Want the truth?
Don't shout and yell
at people – it will
only make them
become defensive

such as minimisation are effective at getting suspects to open up. Houston believes these techniques are permissible, but must be tailored to suit the seriousness of the situation and likely outcome.

“I would encourage parents to avoid using minimisation to the degree that they leave their child feeling they have been hoodwinked. They also don’t want to leave their child with the impression that this is how normal life is handled. This approach is reserved when there is significant deception and the truth is critical to resolution,” he says.

ELICIT THE TRUTH

Unlike Houston, few of us will be faced with situations in which getting to the truth is critical to national security, but there will be plenty of other times when these methods can come in handy. Some useful transition statements to elicit the truth in your personal life include the following:

1. You suspect your partner of cheating on you. ‘Everyone makes mistakes, we’re all human, we all make mistakes. What determines the future is not the mistake but how one handles it.’
2. You suspect your child of hiding something from you. ‘Before you say anything, you need to understand that I need the whole story here. Anything less isn’t going to work.’
3. You feel a colleague has been deceptive. ‘I understand how things happen, however, it would be really helpful for me to have real and candid feedback regarding this situation.’

In all cases, the statement has to be delivered in a respectful and low-key manner. Houston says that we should ‘SEL’ ourselves if taking this approach. That means Slow your rate of speech, Engage by orientating your body and your focus on the person (but not in a challenging way) and Lower your voice by speaking softly.

In short, what you are doing is compelling the other person to move from wanting to deceive you to feeling compelled to tell you the truth. And it is all done without threats or violence.



‘Good cop’ CIA techniques can help you extract the truth from anyone... no matter how young

Jo Carlowe is a science journalist who writes for *The Times* and *The BMJ*.




Listen to *The Truth And Nothing But The Truth*
bbc.in/2z35Rgz

In recent years, the CIA has been accused of using much more brutal methods in its interrogations, particularly when it comes to al-Qaeda suspects following the September 11 attacks.

Torture is prohibited under the Geneva Conventions and in international human rights laws. But perhaps the greatest argument against torture is its ineffectiveness. In December of last year, The Senate Intelligence Committee concluded that the CIA’s ‘enhanced interrogation techniques’ produced either no intelligence or ‘fabricated information’ that resulted in faulty intelligence.

“The lessening of fear by relying on the monologue and short-term thinking is more powerful and effective than instilling or increasing the fear,” agrees Houston.

Indeed, the notion that good cop is better than bad cop is supported by science. A study by Michel St-Yves and Nadine Deslauriers-Varin from the University of Montreal’s School of Criminology found suspects were more likely to confess if they had a good rapport with their interrogator. According to the researchers, getting criminals to admit their guilt is ‘an art form’ that relies on finesse rather than coercion.

Getting physical might elicit a confession of sorts, but it won’t bring you the truth. Convincing a person through charm and guile will. 

ENGINES THAT RUN FROM BODY HEAT



Choose from kit or assembled at
WWW.STIRLINGENGINE.CO.UK



MY BRAIN MADE ME DO IT

A head injury or brain tumour can radically change someone's personality – in severe cases causing them to commit atrocious crimes. How can doctors help rehabilitate them?

WORDS: LINDA GEDDES

The tumour growing in the front of the schoolteacher's brain was the size of an egg. It was the likely source of his recent headaches, balance problems and difficulty writing. But these symptoms paled in comparison to the personality change that the tumour apparently

brought about. Several months earlier, the man had been arrested after making sexual advances towards his prepubescent stepdaughter; he had also amassed a trove of pornography, including indecent images of children.

Although he knew his urges were unacceptable, he claimed that his 'pleasure principle' ➤

GETTY



Brain scan of an Ischemic stroke victim, showing brain cells which have died in the left parietal lobe



overrode his restraint. He also insisted that this interest in children and his compulsion to act upon his sexual urges was new. It was plausible, his doctors concluded: the tumour was growing in the right lobe of his orbitofrontal cortex (a brain area linked to social behaviour, judgement and impulse control) and once it was removed, his deviant sexual urges apparently disappeared.

We often assume that paedophiles or people who commit other atrocious acts are nothing like us; they were either born bad or became that way because of maltreatment during their childhood. Increasingly though, brain injury – caused by a blow to the head, a stroke, or a tumour pressing on neighbouring brain tissue – is being recognised as a factor that can predispose to or trigger the onset of criminality. Sometimes these injuries bring about personality changes so obvious that they raise immediate alarm bells, but often the change is more subtle and the brain injury goes undetected.

It's not only serious crimes like paedophilia or murder that are being linked to brain injury: a recent study of 613 men at Leeds Prison revealed that 47 per cent of them had experienced at least

47 per cent of prisoners had experienced at least one traumatic brain injury, with most of them being injured before committing their first offence

one traumatic brain injury (a serious blow to the head where they'd either lost consciousness or felt dazed or confused) with most of them being injured before committing their first offence.

Not only could the diagnosis of such brain damage result in more effective rehabilitation programmes that reduce reoffending, but by studying the affected brain networks, scientists are gaining new insights into the nature of criminality itself.

PERSONALITY CHANGE

The idea that brain damage could trigger personality change has a long history. One of the first documented cases was that of Phineas Gage, a 25-year-old American railway construction worker who, in 1848, survived an



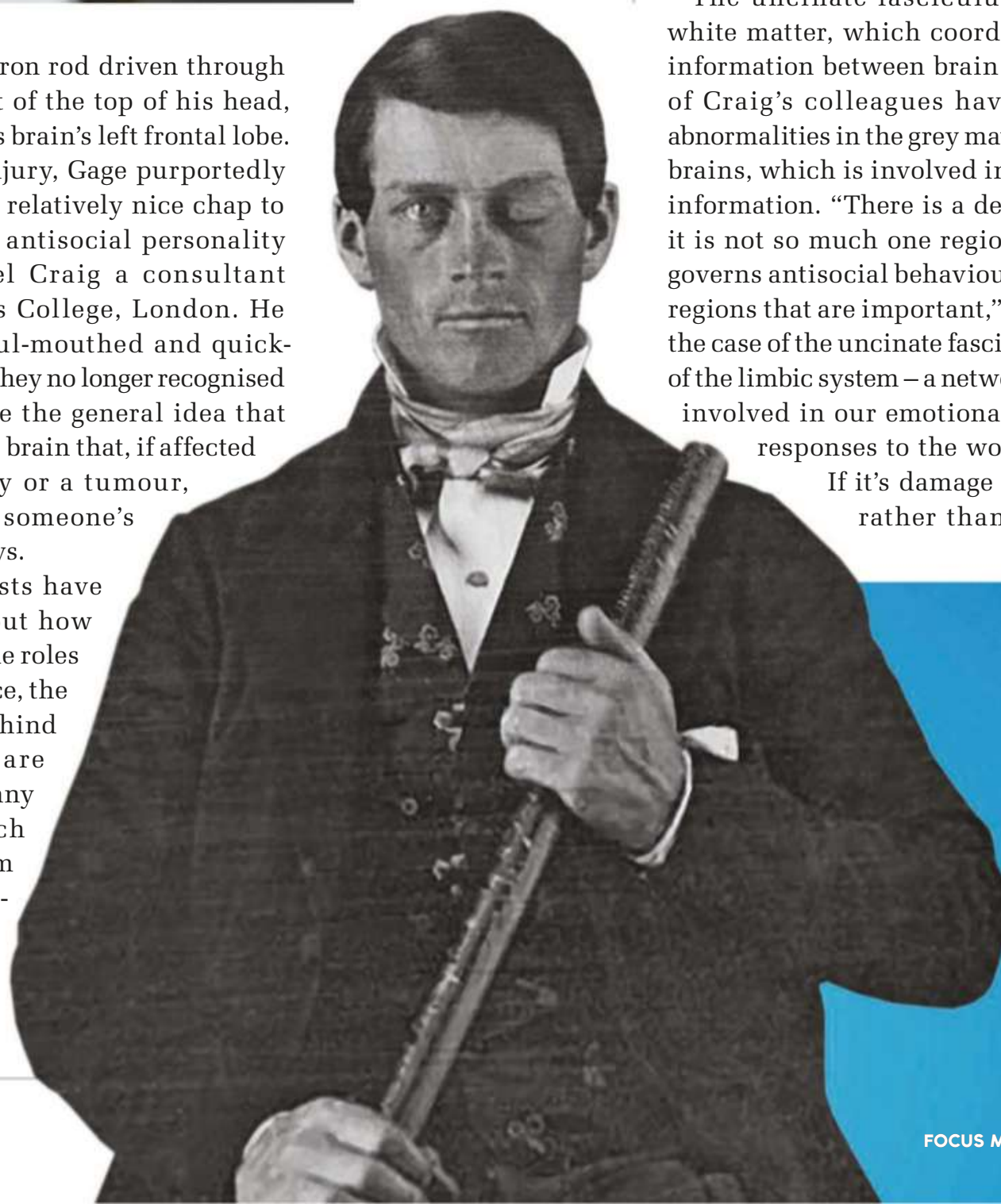
LEFT: The skull is on display at Harvard Medical School and shows the hole in the cranium

BELOW: Phineas Gage who suffered an accident where a metal rod passed through his skull

accident that saw an iron rod driven through his left cheek and out of the top of his head, destroying much of his brain's left frontal lobe.

"As a result of his injury, Gage purportedly changed from being a relatively nice chap to somebody with more antisocial personality traits," says Michael Craig a consultant psychiatrist at Kings College, London. He became stubborn, foul-mouthed and quick-tempered; friends said they no longer recognised him. "From that came the general idea that there are regions of the brain that, if affected by an injury, surgery or a tumour, can actually change someone's personality," Craig says.

Since then, scientists have discovered more about how the brain works and the roles of its parts. For instance, the frontal lobes sit just behind the forehead and are thought to be where many higher functions such as planning, problem solving and decision-making (as well as the regulation of impulses and social behaviour) take place.



They have also studied the brains of people with seemingly more innate antisocial personality traits, such as psychopathy, for clues about what makes them tick. Craig and his colleagues recently discovered abnormalities in the uncinate fasciculus (the 'wires' connecting the frontal lobe to the emotion-regulating amygdala) in psychopaths convicted of violent crimes including rape and murder. "We found that it was bumpier or less well formed than it was in people who didn't have psychopathy," Craig says. The worse their antisocial behaviour, the greater the abnormality seemed to be.

Other researchers have reconstructed the injuries sustained by Phineas Gage using modern imaging and computer software, discovering that he too must have sustained damage to the uncinate fasciculus, as well as extensive damage to the prefrontal lobes.

The uncinate fasciculus is composed of white matter, which coordinates the flow of information between brain regions, but some of Craig's colleagues have also identified abnormalities in the grey matter of psychopaths' brains, which is involved in the processing of information. "There is a developing idea that it is not so much one region or another [that governs antisocial behaviour], but networks of regions that are important," Craig explains. In the case of the uncinate fasciculus, it forms part of the limbic system – a network of brain regions involved in our emotional and behavioural responses to the world around us.

If it's damage to brain networks, rather than specific brain ➔

regions that matters, this could help explain a puzzling finding: “As a neurologist, one of our dirty, little secrets is that often the location of brain damage doesn’t link up with where we think the symptoms are coming from,” says Michael Fox, an associate professor of neurology at Harvard Medical School in Boston. Take Broca’s aphasia, a condition in which people struggle to speak fluently, often as the result of a stroke. It is widely assumed to result from damage to Broca’s area, a small region in the left anterior frontal lobe involved in language processing. But when you scan people’s brains, the damage is often elsewhere. Importantly though, these various brain lesions all connect to the left anterior frontal lobe.

MORAL COMPASS

In the course of his work Fox has linked many such medical symptoms to different brain networks using a map of the human brain’s connections called the Human Connectome. More recently, however, he and his colleagues have

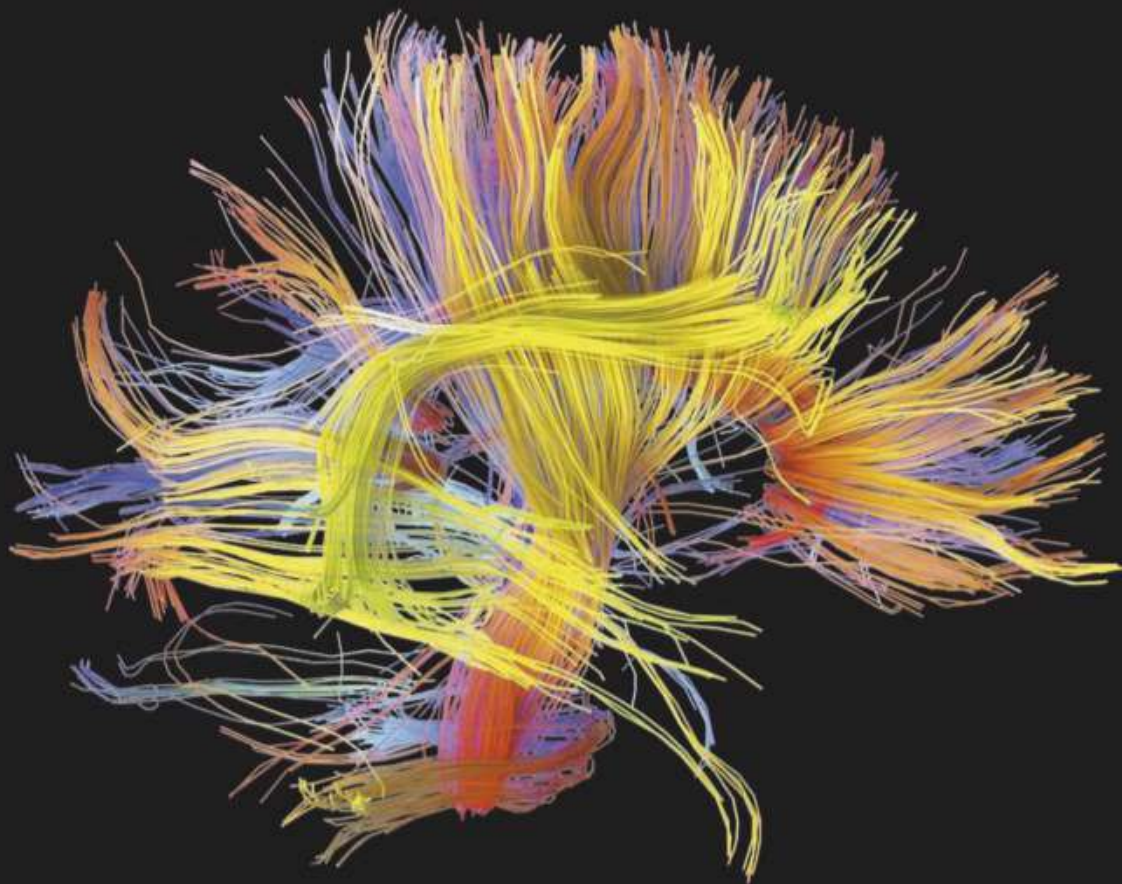
There have been court cases where a defendant’s brain injury has been used as a mitigating factor when determining their sentence

turned their attention to a different symptom: criminal behaviour.

The team searched the medical literature for case reports of patients who had been normal, law-abiding citizens until experiencing a brain injury, such as a stroke, brain bleed or tumour, which apparently prompted them to start committing violent, sexual or non-violent crimes. They identified 17 case reports where the brain images were good enough to be mapped onto the Human Connectome. Even though the damage affected different brain regions in the various individuals, their lesions all mapped onto a common network: one which becomes active when healthy people make moral decisions,




The brain’s frontal lobe is responsible for conscious awareness, and is involved in motor skills, cognitive functions and speech



such as whether it's ok to steal a loaf of bread if your family is starving.

Although the schoolteacher's case wasn't included in their analysis, Fox says he is aware of it. "His lesion location showed exactly the same connectivity profile as all of the other lesions that were included in our network," he says. So too, did the injuries sustained by Phineas Gage.

Fox cautions that many more patients need to be examined before they can be sure of the existence of a brain network that can be reliably associated with criminal behaviour. But if their finding holds true, it could have profound social and legal implications. Already, there have been a handful of British court cases in which a defendant's brain injury or medical condition has been used as a mitigating factor when determining their sentence or their entitlement to compensation. A reliable test would make such decisions easier: "In theory, you could take our network and say 'Does the lesion fall within this network or does it not?'" and if it doesn't it would certainly decrease the chances that that lesion was contributing to the criminal behaviour," says Fox. 

Coloured 3D scan of the bundles of white matter nerve fibres in the brain. The fibres transmit nerve signals between brain regions and also to the spinal cord

Brian Thomas with his wife Christine

SLEEPWALKING KILLERS

Can you be guilty for a murder you committed in your sleep?

When Brian Thomas strangled his wife Christine, in 2008, he claimed to have been in the throes of a nightmare about a 'boy racer' who had broken into the campervan that they were sleeping in, whom he was fighting off. At trial, the judge said Thomas bore no responsibility for his actions, and he was released – although he was advised to seek treatment for his 'night terrors'; a disorder in which people experience sudden and intense dread during sleep, and which, in the most severe cases, is associated with injury to themselves or other people. Thomas was also a frequent sleepwalker.

In such cases, perpetrators can use a legal defence called automatism, which means they had no control over their body at the time of the crime. When people are sleepwalking, their prefrontal cortex – the area of the brain responsible for planning, judgement and impulse control is effectively sleeping, even though other areas are wide-awake.

The automatism defence can't be used if someone did something that caused them to lose control over their body, however. For instance, when a British man called Zack Thompson raped a woman while holidaying in Portugal, his claim that he was sleepwalking was undermined by the fact that he had drunk seven or eight pints before falling asleep.



Brian Thomas with his two daughters at court



ABOVE: Researchers analyse brain activity in offenders
LEFT: Offenders are wired up inside a small room

CONTROLLING BAD URGES

How virtual reality is helping teach patients right from wrong

Inside a small room at a high-security hospital in Montreal, synthetic animations of naked children and adults are projected onto a screen. The men watching them are wired up to devices that track their eye-gaze, the electrical activity of their brains, and the flow of blood to their penises in order to build up a more accurate picture of their sexual preferences than they might be prepared to admit themselves.

Each year, Patrice Renaud and his colleagues assess some 70-80 sex offenders in this way, to help judges assess the risk they pose to society before deciding their sentences.

For instance, not all child molesters are sexually attracted to children – sometimes their offence is prompted by another mental health problem – an important distinction to make in terms of their treatment. “Virtual reality enables you to simulate every possible context that you could imagine, which is a major asset when you’re talking about criminal behaviour,” Renaud says. “When the avatar is mimicking a child, the individual that we assess has the impression of being seated in front of a real child, which is more potent as a stimulus than using 2D pictures.”

In the future, he believes virtual reality could also play a role in the rehabilitation of sex offenders. It could be used to teach offenders about how their brain responds to certain situations, or to help them develop skills they’re deficient in, such as empathy.

Already, this is being tested in the context of domestic violence. At the University of Barcelona, first-time offenders undergoing a community rehabilitation programme are offered a session in which they embody a female avatar who encounters an aggressive male. He criticises their appearance, smashes a phone against the wall and then advances towards them, invading their personal space. After the session, the ability of perpetrators to recognise signs of fear in female faces improved.

“An important aspect of treating someone is that they will be able to use the skills you teach them in the real world,” explains Renaud, who isn’t involved in the Spanish research. “If you learn in virtual reality that you can feel something for an avatar, or that you can’t get too close to an environment or a bad thing will happen – then the trainee is more likely to transfer those lessons into real life.”

It also raises questions about how such individuals should be managed: “When you start talking about patients with brain lesions that are associated with criminal behaviour, are they criminals or are they patients?” asks Fox. “And if they are patients, should they be incarcerated, or should they be treated?”

PRISON OR PRESCRIPTION

Further down the line, such research could prompt further questions about how to handle criminals with more subtle abnormalities in the same brain networks, perhaps arising during development, or due to childhood neglect. “Do we treat them as criminals who need to be locked up, or do we treat them as patients in need of treatment?” asks Fox.

For now, that question remains a largely theoretical one: there isn’t yet an effective treatment for adult psychopathy, for instance. But as we learn more about the changes underpinning antisocial behaviour, the chances of finding one grow stronger.

Similar questions often cross Ivan Pitman’s mind. A clinical psychologist who has spent his career working with offenders – some of them detained in Ashworth High Security Hospital on Merseyside – his research suggests that undiagnosed brain injury may be a contributing factor in many more criminal cases than is widely recognised. It may also be impeding rehabilitation efforts.

Ashworth houses some of the UK’s most violent prisoners; men whose criminality is

judged to stem from mental illness – a chemical imbalance in the brain, which could potentially be corrected with drugs. However, Pitman wonders if, in some cases, it might arise from physical brain injury that is less reversible: “Once brain tissue is dead, it’s dead. The brain copes by finding new pathways for signals to go around, but it is never as effective as it was before,” he says.

He and his colleagues have been reassessing some of Ashworth’s most difficult inmates using a combination of cognitive tests and brain scans: this revealed that many of them had previously undiagnosed injuries to their brains.

This doesn’t necessarily excuse their bad behaviour; after all, there are plenty of people with brain injuries who don’t commit crimes: “Brain injury does not inject criminality or antisocial behaviour. But what it can do is remove some of the inhibitors,” explains Pitman.


Even so, viewing an inmate’s behaviour through the lens of brain injury can be helpful. “It means that we can start to look at things much more functionally. Not that this person is bad, or is trying to upset or annoy you, but actually, perhaps this person doesn’t quite understand what is expected of them, and doesn’t quite understand the things that you understand,” says Pitman.

“Are they criminals or are they patients? If they are patients, should they be incarcerated or should they be treated?”

It also has implications for their treatment: People with brain injuries can often come across as quite normal during conversation, but may struggle to fully comprehend what people are saying to them; or find it difficult to multi-task, set goals or make decisions.

When someone who hasn’t committed a crime sustains a brain injury, they will be assessed by a team of psychologists, occupational therapists and physiotherapists to identify such deficits and develop strategies to help them function in everyday life. Such assessments aren’t usually done when someone is sent to a secure hospital or prison, but their treatment and rehabilitation often hinges on psychological interventions, such as relaxation techniques and talking therapies, which require engagement if they’re to be effective. “We have to acknowledge that this way of treating them may not work very well because they’re not able to learn and respond in the way that healthy people are,” says Pitman. “Our job is to identify the obstacles they face and find ways of overcoming them.”

Pitman’s current focus is on the general prison population. As his study of inmates at Leeds Prison revealed, up to half of prisoners may have experienced a brain injury in the past. And although many of these injuries are mild, an estimated 15 per cent are moderate or severe, which means those affected may be struggling with everyday tasks.

Brain injuries can’t be fixed, but given the right environment, people can learn to work around them to some degree. As Pitman says: “By failing these people, there’s a risk of further victims being created.” 



Listen to the story of a man whose night terrors became so violent his wife made him get help
bbc.in/20GZvbv

Psychotherapy sessions could help rehabilitate inmates



Linda Geddes is a science writer and author. Her new book *Chasing The Sun* is out in January.



GETTY

RECEPTION



GETTY

DETECTION

Should we be turning to brain scans to help us
decide whether criminals are lying in court?

WORDS: HAYLEY BENNETT



The day before New Year's Eve 2009, the temperature in Massachusetts dropped below -10°C. Most people would have been holed up indoors with family, enjoying the festivities. Not Lorne Semrau. The 63-year-old Tennessee psychologist, who was due to stand trial for fraud the following year, was on his way to Framingham that day to get a brain scan.

There was nothing wrong with his brain as far as anyone knew. No, this was an exercise in collecting evidence. Semrau's attorney had arranged for Stephen Laken of the Cephos Corporation to carry out a test that would involve recording Semrau's brain activity in a functional magnetic resonance imaging (fMRI) scanner and looking for signs of deceptive thoughts. In other words: he was going to have a high-tech lie detector test. The stakes were high. Semrau hoped to clear his name, while Laken wanted to get his name on the first court case to allow fMRI lie detection results as evidence.

They met at 6am, talked over the procedure and then Semrau climbed onto the scanner bed. While the machine scanned his brain, Semrau responded to a series of questions about the psychiatry bills that led to the fraud charges, as well as a bunch of other ones such as "Is today Tuesday?" and "Have you ever lied to a court?" It was an exhausting procedure and by the end Semrau was finding it hard to read the questions, which were flashing up on a screen in front of his face. He had to return in January to re-do part of the test.

So what happened? Well, in short, the court didn't admit the brain scans and Semrau was ultimately found guilty on three counts of fraud. In an appeal in 2012, the court ruled again that

the fMRI results could not be admitted. However, the case sparked an ongoing debate about the technique and whether it could and should be used in criminal cases. It also triggered what's called a 'Daubert' hearing in the US – where the court decides if a novel type of evidence can be admitted, based on meeting a certain standard of scientific rigour.

As James Giordano, a neuroethicist at Georgetown University in Washington DC explains, "To this date, the use of fMRI, together with other forms of neuroimaging, has not fully met the Daubert Standard for admissibility into court." In particular, he says, it still hasn't been used to determine whether someone is guilty or not guilty. That could change in the future

though, if lie detection techniques improve to a level that satisfies the courts. Whether they *should* be used is another matter.

The debate around the controversial fMRI technique is framed by a parallel debate about polygraph tests. These are what we traditionally think of as lie detector tests. Introduced about a century ago by John Larsson, a Californian police officer, they have

changed relatively little in that time. Essentially, polygraph tests take simple measures, such as pulse rate, blood pressure and sweat on the palms, and use them to determine whether someone is lying or not. However, polygraph tests are not used by the US courts either and in some states are actually banned from being admitted as evidence because they are not considered accurate enough.

Even so, polygraphy is still used in contexts where there could be legal implications, such as in governmental job screens. In the UK, convicted sex offenders are given lie detector tests to check whether they are breaching the conditions of their probation. While certain studies suggest that this has resulted in offenders

**That could change
if lie detection
techniques improve
to a level that
satisfies the courts
– whether they
should be used is
another matter**



GETTY X2



LEFT: A man undergoing a traditional lie detector test with a polygraph machine

BELOW: MRI (Magnetic Resonance Imaging) brain scans



being more likely to report bad behaviour, in general, scientists are sceptical of the accuracy of polygraph testing.

Nevertheless, Ministry of Justice figures released last year show that, since 2014, 166 sex offenders who took traditional lie detector tests were sent back to prison. “What the authorities have been saying is ‘we won’t bring this evidence to court, but it’s a reason why, if you’re out on probation, you might be called back in,’” says Paul Catley, who studies neurolaw at the Open University. He adds that, as in some states in the US, there is nothing written in law to stop the courts admitting lie detector evidence. So far, though, they haven’t.

It might take only one case where polygraph results are used as evidence to set a precedent for future cases. And the same would be true for brain scans, say if another Semrau case came up and had a different outcome.

BRAIN DAMAGE

Neuroimaging is already creeping into the courts for other reasons. MRI scans aren’t currently used to detect deception but they are used, for example, to show if a defendant had a brain injury or disease that could explain their behaviour. See page 55.

In 2015, Catley and Open University colleague Lisa Claydon carried out a search for ‘neuroscientific evidence’ on all the cases brought to the Court of Appeal between 2005 and 2012. (Because trials are not publicly reported in the UK, they were limited to appeals.) They found 204 cases in which neuroscientific evidence was used by the defendants. This included 21 cases using MRI scans and 17 using CAT scans.

Claydon recounts one instance they uncovered where an MRI scan was ordered in an appeal after a trial involving a father and son. The father maintained his son had suffered a severe head injury for which he was wrongly accused of making fraudulent claims to the Criminal Injuries Compensation Board. In the original trial, the court had found there was no evidence of any brain damage. “What emerged over the years that followed was that, actually, he had a degenerative brain disease,” says Claydon. “The problem in that kind of ➤

case is that psychologists giving the expert evidence are worried about malingering – the defendant who says they’ve got dementia and miraculously recovers from it. So, in those cases, some physical evidence that can pinpoint that there might be an organic cause in the brain could be really useful.”

The question now is whether brain-imaging techniques could be used by the courts in lie detection. Could they, muses Giordano, “supercede” polygraphy and, with some refinements, reach a level of accuracy that older lie detectors will never achieve? “The intent is to have something better than the polygraph, not necessarily as a standalone measure but certainly that can be used in concert with other approaches so as to... make suggestions about an individual’s [honesty].”

In a 2017 article in *The United States Law Week*, neurolaw professor Owen Jones and judge Morris Hoffman predict “significant increases in accuracy” of lie detection by neuroimaging in the next 30 years. This is certainly a positive outlook from Jones, as the

scientist who wrote the report for the Daubert hearing in the Semrau case. At that time, each scan took roughly 16 minutes and was conducted while Semrau answered a series of questions about the alleged frauds. So it gave only an overall impression of Semrau’s ‘truth-telling’ in response to a whole series of questions – a sort of average of honesty. It couldn’t pick out an individual lie. In addition, Laken himself testified that the technique had a “huge false positive problem”. In other words, although it was good at detecting lies when people were lying, it also detected a lot of lies when people were telling the truth.

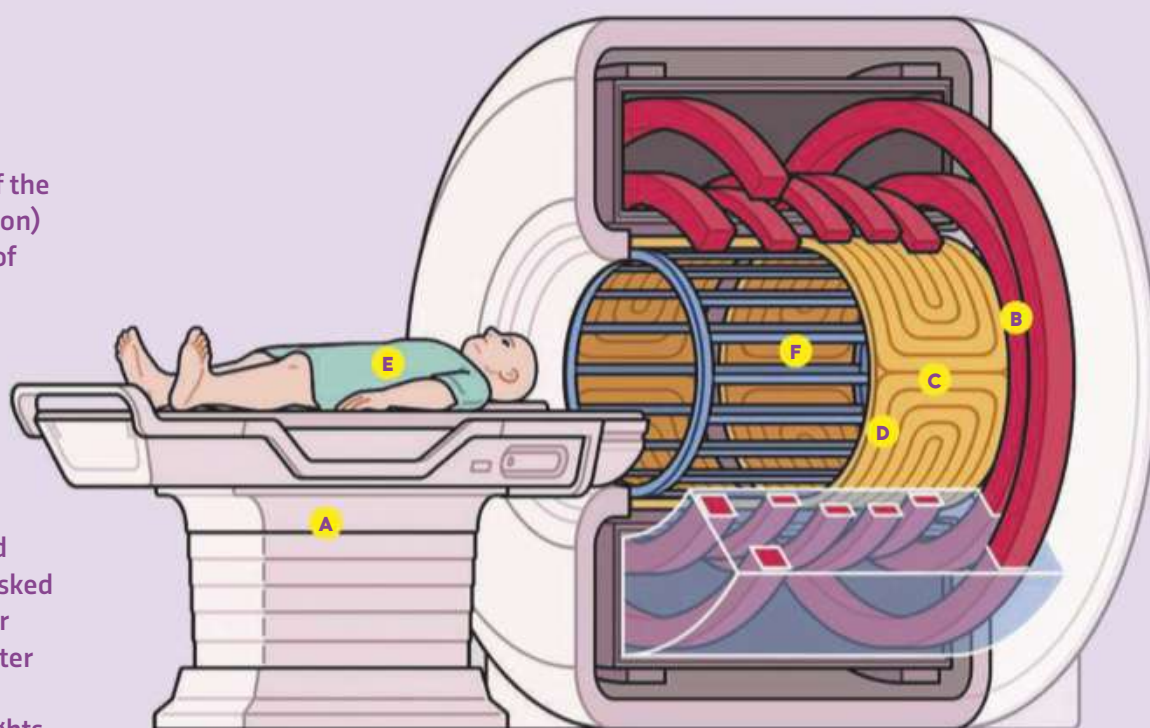
IN THE REAL WORLD

Another criticism commonly levelled at fMRI is that it has never been tested in real-world settings, only in the lab. This was one of the key reasons given for the fMRI evidence being dismissed again in Semrau’s 2012 appeal. As Catley notes, being asked questions in a scientific experiment is totally different to having to defend yourself in a criminal trial.

HOW IT WORKS

MRI SCANNER

Magnetic Resonance Imaging (MRI) takes advantage of the fact that the nucleus of a hydrogen atom (a single proton) behaves like a weak compass needle. In the presence of a strong magnetic field, the hydrogen atoms will align themselves, but a radio signal of the correct resonant frequency will cause them to deflect slightly. When the signal is removed, the atoms return to their equilibrium state and emit a radio signal of their own. The machine collects the signals from oxygenated and deoxygenated blood in the brain, which give slightly different signals. Oxygenated blood indicates increased brain activity. In a lie detection test, the defendant is asked questions relevant to the case during the scan, in order to measure the effect on brain activity levels. A computer interprets the results and produces an image. Certain patterns of brain activity may indicate deceptive thoughts.



A. Scanning table

The patient can only be scanned from inside the magnetic coil, so a motorised table slides them in and out.

B. RF system

An antenna produces a radio signal to ‘nudge’ the hydrogen nuclei and listen to the answering radio wave they emit.

C. Liquid helium

Liquid helium is pumped through an enclosing jacket to cool the super-conducting magnets almost to absolute zero.

D. Main magnet

Superconducting magnetic coils produce a magnetic field of 1.5 teslas – that’s about 300 times stronger than a fridge magnet.

E. Patient

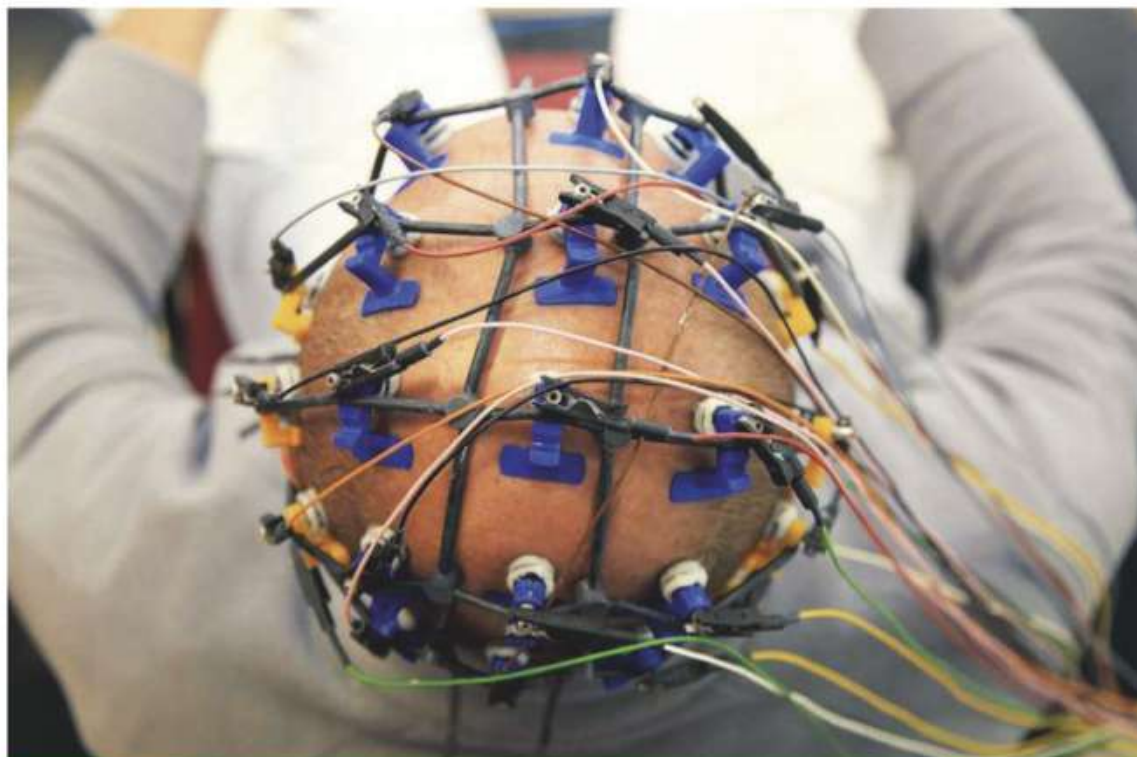
The high magnetic fields mean patients with cochlear implants, pacemakers or embedded shrapnel usually can’t be scanned.

F. Gradient system

A second coil distorts the main magnetic field so that the resonant frequency of the protons varies according to position.

“You are being accused of a crime and you have all the anxiety around that and you might have other reasons to want to conceal evidence, all of which may be affecting your brain processes as you respond to a question.” Also, just like with a polygraph test, there’s the possibility that the person taking the test really believes something that is false, in which case it’s not clear whether the machine would detect it as an honest statement or a lie.

Add to all of this the fact that fMRI tests can be derailed by minor head movements, wiggling your fingers, being tired, or thinking about anything besides the question you’re being asked, and the case for fMRI lie detection looks a bit flimsy. Yet, Jones and Hoffman expect to see increases in accuracy due to improvements in the imaging technologies themselves, as well as the pattern recognition algorithms used by computers to analyse their outputs. If and when fMRI lie detection reaches higher standards of accuracy and reliability, they say judges will have to be prepared to admit the results as evidence in court. Initially, some courts may decide that the scan techniques match up to the Daubert Standard, while others may not.



THE THOUGHT POLICE

Aditi Sharma is currently serving a life sentence in an Indian jail for murdering her ex-fiancé. She was convicted a decade ago at least partly on the basis of an EEG test – the type that involves wearing a skull cap with wires sticking out of it. She didn’t need to say anything during the questioning, because the electrodes on her skull were designed to read her thoughts. Although scientists


internationally have expressed doubts, Indian police have now used skull caps to conduct something called the Brain Electrical Oscillations Signature (BEOS) test in over 1,000 forensic cases, according to a 2017 paper by Indian researchers. They claim the BEOS test is able to distinguish the brain’s response to events that it remembers versus those that it doesn’t.

It had a huge false positive problem – it also detected a lot of lies when people were telling the truth

In fact, getting the technology into the courtroom may be just the first hurdle; there will be some major issues around consent to overcome. As fMRI involves looking inside someone’s brain, it will be more complicated than simply asking a defendant to consent to a scan. They will also need to consider what happens if there’s an ‘incidentaloma’, says Giordano. “If during this brain imaging other things are found, how will this information be handled?” Not only is there the issue of what a scan might reveal to a patient about their health, but also about how to protect the patient from

that information being misused if it enters the public record. Law student Stephanie Kostiuk foresaw this issue in a 2012 thesis calling for a Neuro Information Non-discrimination Act to prevent employers from discriminating against people on the basis of their brains.

Finally, there’s the money problem. When Catley and Claydon did their research, they stumbled upon a number of cases in which rich people were employing neuroscientists as experts to make certain pleas. “They weren’t all backed by MRI scans,” says Claydon, but she does suggest that being ‘moneyed’ will always help in a court case, and no less in an era of neuroscientific evidence.

As for Semrau, he was sentenced to 18 months in prison and died peacefully at home in 2016. Of course, we’ll never know whether the fMRI evidence would have made a difference had it been admitted. But as Giordano points out: “Although the criticism has been that we haven’t done this in the real world, it doesn’t necessarily mean that we can’t.” 

Hayley Bennett is a science writer based in Bristol.

HACKERS

CAN THEY BE BEATEN?

The rise of the internet has transformed hacking into an opportunity for crime, activism and political interference. So who are the hackers and can they be stopped?

WORDS: CHRIS HALL

The last couple of years have been rife with speculation. The Trump administration is still under suspicion for colluding with Russia during the 2016 presidential election. US intelligence agencies concluded that Moscow attempted to sway the election in favour of Trump. Russian hackers supposedly stole information linked to Hillary Clinton's campaign, which Wikileaks then released to undermine her. Whether Trump was privy to this is still a matter of debate.

Across the Atlantic, hackers were also at work during the 2017 French presidential elections. Eventual winner Emmanuel Macron and his En Marche! party were victims of a 9GB leak of emails, just 48 hours before the voting took place.

Here in the UK, in May 2017, hackers used the WannaCry ransomware worm to cripple computer systems in 40 NHS hospitals.

In the wake of each attack, politicians spoke urgently of the need to 'regulate' the internet. Across the West, our democracy and our freedom are under sustained attack, and at the heart of the battle is our grasp on technology.

That might sound like hyperbole, or even the stuff of a movie trailer. But, consider this: the average person in the UK spends 25 hours a week online and has between 27 and 40 online accounts. There are set to be 20 billion connected devices in the world by 2020 – and, in 2016, in the US alone there were more than 1,000 recorded data breaches. Hacking isn't just about pinching passwords any more: the geeks have truly inherited the Earth.

"There's no question that there is more malware now than there has ever been," says David Emm, principal security researcher at antivirus and internet security specialists Kaspersky Labs. "And the volume is growing massively. We analyse a million objects [of malicious code] per day in our virus lab, and more than ➔

60 per cent of our detections are of code that has never been seen before.”

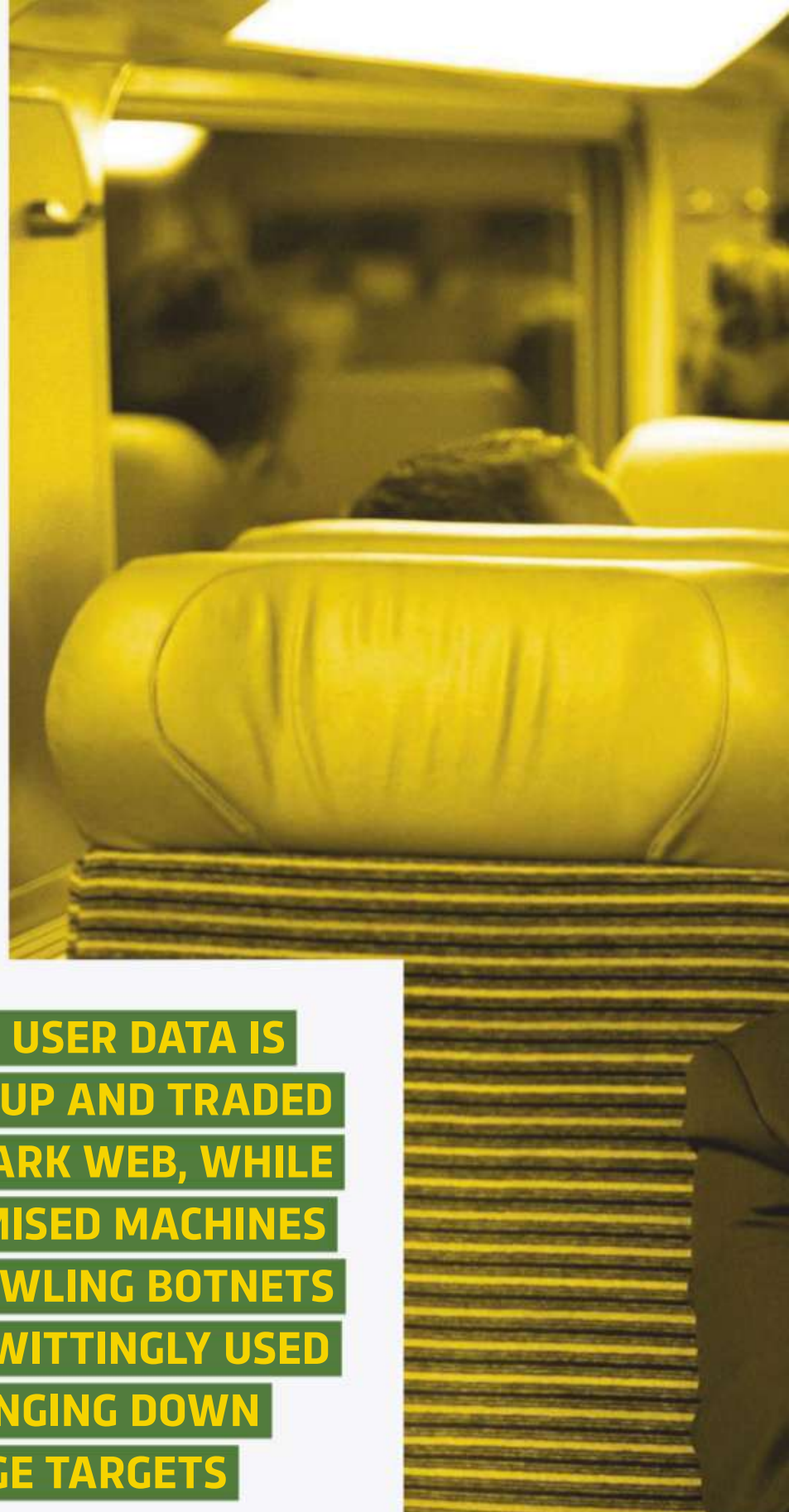
Such a proliferation of threats is undeniably concerning, but also hard to grasp. One reason the subject of hacking can feel so nebulous is that the term covers a multitude of sins. Cybercrime attacks can be serious offences such as theft, extortion, espionage, libel or fraud, but they can also be low-level nuisance behaviour. Where this comparison with real-world crime differs is that every hack and every leak can feed into greater crimes. For example, stolen user data can be bundled up and traded on the dark web (the dark web refers to encrypted sites that cannot be found using standard browsers or search engines), while compromised machines join sprawling botnets to be unwittingly used in bringing down large targets.

CYBERCRIME VICTIMS

Let's take a look at the NHS ransomware attack as an example. It was carried out using tools leaked online by nefarious group the Shadow Brokers. The tools were recognised by the international security community as hailing from the Equation Group cyberwarfare team, thought to be affiliated to the National Security Agency (NSA). They contained a number of 'zero-day exploits', which could be used to gain access to computers running Microsoft operating systems from Windows 2000 to Windows 8. The toolkit – known as Eternal Blue – exposed a multitude of vulnerabilities

RIGHT: Hackers targeted Emmanuel Macron just 48 hours before French voters were due to go to the polls – he still beat his rival Marine Le Pen to become president of France

FAR RIGHT: There are allegations that Russian hackers interfered with the US electoral system. Some claim this led to the defeat of Hillary Clinton in 2016's US presidential election



**STOLEN USER DATA IS
BUNDLED UP AND TRADED
ON THE DARK WEB, WHILE
COMPROMISED MACHINES
JOIN SPRAWLING BOTNETS
TO BE UNWITTINGLY USED
IN BRINGING DOWN
LARGE TARGETS**

TYPES OF HACK

Don't know your Trojan from your worm? Brush up on your hacker lingo here



VIRUSES AND WORMS

Most malware tends to be either a virus or a worm. The difference comes down to the software's ability to propagate. Like their biological namesakes, computer viruses require a host body, whereas worms can spread from one machine to the next unaided.



DDOS

Short for distributed denial of service, a DDOS attack is basic yet effective. It works on the principle that if a website's DNS server can be overwhelmed by traffic requests, the site will crash. Hackers run botnets – networks of zombie computers or devices – to besiege a server from multiple fronts simultaneously.



GETTY X2



and made it child's play for the perpetrators to spread the WannaCry ransomware around the world.

Where it gets murkier is when you start to consider the motive for the WannaCry attack. It would seem to be financial, yet relatively little cash was paid out – just \$126,000 (approximately £97k) worldwide. This was easy to track, thanks to the open nature of the Bitcoin transactions that were used for payments. And the attack was relatively easily halted by a security researcher who inadvertently realised that by registering a domain name found within the malware, he had activated a built-in 'kill switch'. This ➔



TROJAN

As its name suggests, a Trojan is a form of malware that sneaks into your computer under an innocuous guise (like an email attachment). Its cargo can be any form of malware. A Trojan's specific ability is getting in, then leaving a backdoor open for others to follow undetected.



RANSOMWARE

This subset of malware made the headlines with 2017's WannaCry attack, but has been around since at least 2012. It searches for important files, encrypts them and demands a ransom (usually paid in Bitcoin) for their safe return. In some cases, the ransomware can lock down a machine rather than specific files.



SPEAR-PHISHING

An evolution of phishing (the spelling harks right back to early phone-based hacking, or 'phreaking'), spear-phishing is more direct and consists of targeted campaigns, usually over email, to spread malware in a particular network or company. The messages sent out would be laden with Trojans.

THE BIGGEST HACKS IN RECENT HISTORY



MACRON EMAIL LEAK

Just 48 hours before the run-off poll between Emmanuel Macron and Marine Le Pen, a 9GB cache of emails from Macron's En Marche! party was posted on PasteBin, a filesharing platform. They were spread to WikiLeaks. "The attacks were so simple and generic that it could have been practically anyone," France's cybersecurity chief said.

BANGLADESH BANK HEIST

In February 2016, hackers got the login credentials used by Bangladesh Central Bank for the international banking transfer system SWIFT. They tried to transfer \$951m to accounts in Sri Lanka and the Philippines. Most transactions were flagged, but \$101m was removed. A Trojan known as Dridex was used, which hides in MS Word or Excel attachments.



WANNACRY ATTACK

On 12 May 2017, a global ransomware attack affected more than 230,000 computers, including those of the NHS, FedEx and German train operator Deutsche Bahn. The malware was leaked from the NSA, and targeted machines running Windows XP and Windows 2003. The attack yielded just over \$126,000 in payments and caused considerable upheaval.

YAHOO! BREACH

In 2016, Yahoo! was forced to confirm that its systems had been breached twice, in 2013 and 2014, resulting in the loss of more than a billion users' personal information, including passwords. The hackers used fake browser cookies that allowed them to dupe the site's login systems. To date, it is the largest loss of customer data by any single company.

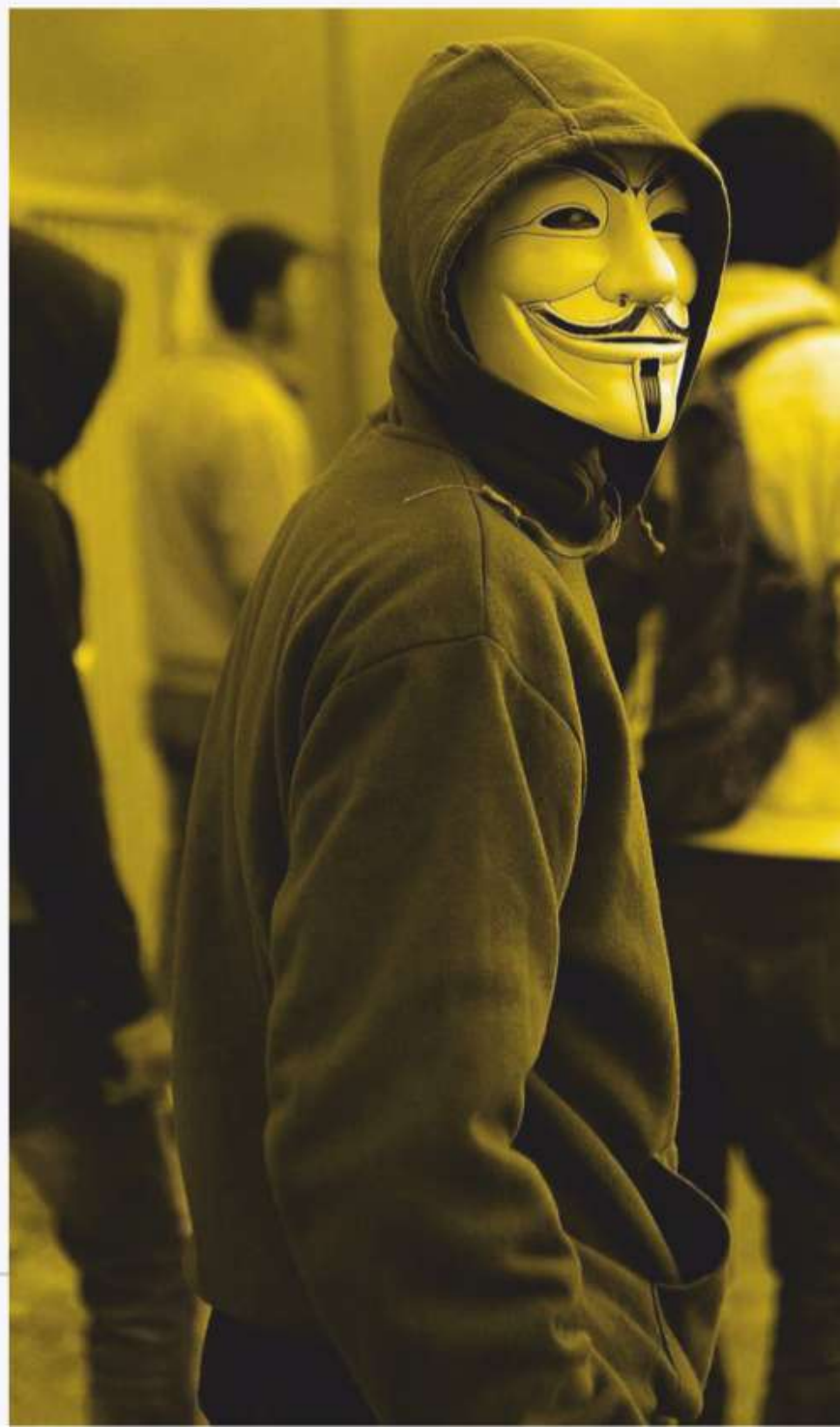


CHIPOTLE ATTACK

The Mexican restaurant chain, which has more than 2,250 outlets in the US, reported that if you paid with a credit card between 24 March and 17 April 2017, your credit card details had almost certainly been obtained by hackers. The attack vector has not been confirmed, but the malware involved allegedly read the card data directly from the machines as they took payment.

doesn't tally with the sophistication of the tools that were used in the attack, or the capabilities of those alleged to be behind it (some have pointed the finger at North Korea).

So how did we get to a point where hackers can rob and extort with impunity, and – if analysis is to be believed – nations such as Russia or North Korea can interfere in political campaigns? Russian president Vladimir Putin came close to conceding that Russian elements could be behind recent political hacks. "If hackers are patriotically minded, they start to make their own contribution to what they believe is the good fight against those who speak badly about Russia," he said in an interview. (Those with longer memories will point out that interfering in the elections of satellite states was a favourite activity of the US during the 1980s – it just wasn't done online.)



One side of the answer is the exposure of people to the internet. As the Internet of Things grows, we are adding ‘attack vectors’ to our lives. We are opening more and more doors for hackers to walk through. “Smart home technology has not yet been universally adopted, so attackers don’t have much to gain from it other than nuisance value,” explains Emm. But that may soon change when smart home technology reaches a tipping point, and the weaknesses are there to be exploited.

“Companies who have never had to think about internet security in the context of standalone products wake up to the need for security when they add Internet of Things functionality,” says David Harley, a security consultant and chief operations officer for the Anti-Virus Information Exchange Network.

**“BACK WHEN I STARTED,
IT REALLY WAS THE
WILD WEST OUT THERE.
AND THERE WAS AN
INNOCENCE TO IT. WHEN
GROUPS OF US MET IN
CHATROOMS, WE DIDN’T
REALLY REALISE WE
WERE CREATING
CRIMINAL GANGS”**

Although, he adds, the smart home’s sheer scale could also act in its favour. “Because of the wide diversification of brands, technologies and devices, the scope of an individual attack may be comparatively restricted.” Restricted or not, there is the potential for some creatively unpleasant hacking. “Imagine a ransomware attack linked to your heating system,” says Emm.

So you may not have to worry about someone hacking into your smart kettle yet. But that’s only because there are easier ways for criminals to get what they want, whether that’s by simply buying leaked data, sending out a few thousand phishing emails, or exploiting existing vulnerabilities that go unfixed by users who neglect to update their software.

BLAME GAME

But we can’t place all the blame on lazy individuals or companies. The majority of security researchers concur that without punishment, crime is allowed to flourish.

“It is a myth to think criminals have some magical edge,” says Stephen Cobb, senior security researcher at antivirus specialists ESET. “Right now it appears that way with cyber criminals because of the massive failure of governments to mobilise international law enforcement. How many culprits involved in watershed breaches have been brought to justice? Clearly, not enough to deter new entrants to the field.”

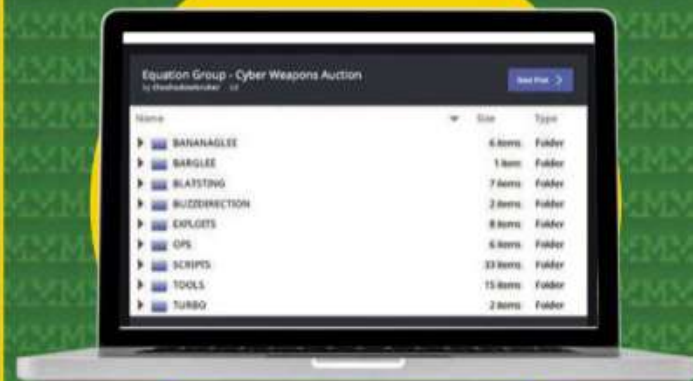
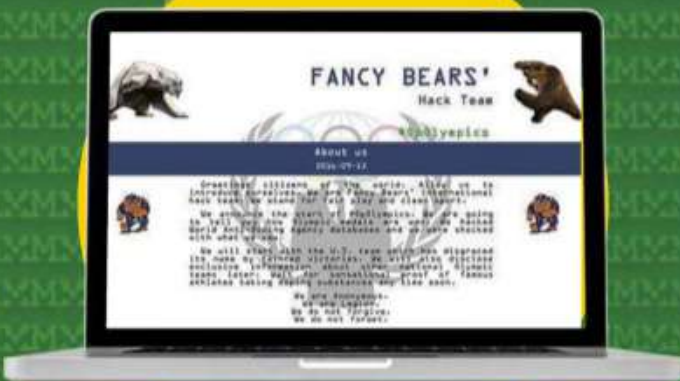
But who are these hackers anyway? The security community is generally cagey about attributing attacks to certain groups or countries, seeing it as the responsibility of law enforcement to act on their pure analysis of the code. Nonetheless, the anonymity offered by the internet makes it hard to be certain. The few major hacking groups that are known to security researchers are the exception, not the rule, and their actual membership can be even harder to pin down.

Cal Leeming gained notoriety as the UK’s youngest convicted hacker in 2007. According to Leeming, his natural talent was “given a bit too much freedom”. He was carrying out illegal

‘Hactivist’ group Anonymous tend to attack religious and political groups, as well as large corporations. Many members opt to wear the stylised Guy Fawkes mask

THE BIG PLAYERS

Who are the most notorious hacking groups out there and what do they want?



FANCY BEAR

Also known by a myriad of aliases including Sofacy, APT28 and Pawn Storm, this highly capable group is widely believed to operate with at least the tacit approval of the Russian government. It has claimed responsibility for attacks on NATO, the White House, the French election, the US's Democratic National Committee and the German parliament.

LAZARUS GROUP

This group is known for the attacks on Sony Pictures and the Bangladesh Central Bank in 2014 and 2016, respectively. The Lazarus Group is also thought to have attacked the South Korean government between 2007 and 2013. Specialising in financial attacks and espionage, the group has been linked by researchers and the media to the North Korean regime, albeit not conclusively.

SHADOW BROKERS

One of the newest groups to emerge, Shadow Brokers published leaked hacking tools from the NSA in summer 2016, with the possible assistance of a former military contractor at American IT consultants Booz Allen Hamilton. Little is known about the group's identity or motives, but there is speculation that the leak's main purpose is to send a message of mutually assured destruction if the US were to retaliate for the group's hacks on the Democratic National Committee in 2015 and 2016.

UNITED CYBER CALIPHATE

The UCC, also referred to as the Islamic State Hacking Division, refers loosely to all groups claiming to further the ideology of ISIS. Yet it is not known how coordinated it is with others, such as the Tunisian group that claimed responsibility for an attack on the NHS in February 2017. The group has attacked American, British and Australian targets.

EQUATION GROUP

Classed as one of the most advanced threats by security companies, the Equation Group (named for the complexity of its encryption) is commonly believed to be affiliated to the NSA and has been particularly involved in cyber attacks across the Middle East. One such attack was the Stuxnet worm, which destabilised Iranian nuclear centrifuges.

attacks at the age of 12, then in 2006 he was sentenced for using stolen credit card data to buy £750,000 worth of goods. Now running his own security consultancy for high-net-worth individuals, he laughs when asked if hackers really fit people's image of them.

"Stereotypes do generally exist for a reason," he says. Still, he doesn't quite live up to them, as his childhood hacking was borne of a need to support his family, rather than a desire for mischief. "Back when I started, it really was the Wild West out there. And there was an innocence to it. When groups of us met in chatrooms, we didn't really realise we were creating criminal gangs. I used to think the internet should be totally free – no rules, everything goes," he explains. "But we have got to a point where the internet, and anonymity in particular, has brought out the very worst in our culture. It has brought out the best too, but we have become desensitised to how awfully we're treating each other."

As an emerging hacker, Leeming lacked guidance but also felt that the law was too heavy-handed. "It has criminalised schoolkid mischief," he says. He cites the tendency of small crimes to turn into bigger ones. "We need people who can interact with those kind of young adults – people who otherwise develop no grasp of ethics or personal responsibility."

However, the general consensus among experts is that hackers and hacking are things we need to accept will never disappear, yet that doesn't mean we have to give up the fight.

"There will always be some level of criminal hacking, but it is possible to improve human behaviour. For example, there's a lot less crime in America and the UK today than there was 25 years ago, and not because all the criminals have gone online," says Cobb.

When the diagnosis is as all-encompassing as a global issue like cybercrime, so the treatment for it needs to be pretty far-reaching. For David Emm at Kaspersky, it's an education issue.

"Cyber attacks are often reliant on humans and their mistakes, so big businesses could

**"THE BIG TECH COMPANIES
NEED TO TAKE A STEP
BACK AND REALISE THAT
THEIR FUTURE PROFITS
ARE IN SERIOUS JEOPARDY
IF WE DON'T IMPROVE
CYBERSECURITY
ACROSS THE BOARD"**




Watch *Data Detectives* investigating AI software being used by police to assist in custody decisions
bbc.in/2OuZYgK

go a long way towards dealing with the problem by focusing more on a culture of awareness and developing education," he says. "It's like parenting, you can't expect to tell your kids not to do something once and they'll never do it again. It's a

longer-term process."

However, there's no question that serious vulnerabilities remain. "I think the big tech companies need to take a step back and realise that their future profits are in serious jeopardy if we don't improve cybersecurity across the board," says Cobb. "There are massive tech companies sitting on billions in cash and I would argue a chunk of that cash came from the corner-cutting we have done so far."

But that doesn't mean it's all doom and gloom. It's a glorifying myth, says Harley, to think of it as "genius hackers versus plodding security companies". Instead, if we think of hackers like ordinary criminals and guard against them in the same way, then there's no reason why society, including the public, the media, companies and governments, cannot keep cybercrime under control. 

Chris Hall is a science and technology journalist who has written for *Esquire*, *Men's Health* and *GQ*.



Each attack was random. But what if within lists of attacks there was a hidden pattern – information lurking within the statistics?

CAN MATHS

DEFEAT

TERRORISM?

Mathematicians are finding patterns in apparently random acts of terrorism that may provide clues as to how we can thwart such attacks *before* they take place

WORDS: ANDY RIDGWAY

Barcelona, 17 August: 13 dead. London, 19 June: one dead. London, 3 June: eight dead. Manchester, 22 May: 22 dead. Paris, 20 April: one dead. Stockholm, 7 April: four dead. London, 22 March: five dead. So goes the list of terror attacks and the number of lives claimed across the UK and Europe in 2017. Each attack was shocking, unpredicted and random. But what if within lists of attacks like this, the cold, hard data of terrorism, there was a hidden pattern – information lurking within the statistics?

It's a question that came to physicist Professor Neil Johnson at the University of Miami while he was visiting Bogota in Colombia in the 1990s. Since the mid-'60s, the country has been in the grip of a conflict between the government and a host of insurgent groups. "I'd turn on the news and three were killed today, then no one, then five, then two, then six," says Johnson. "It's a complicated set of numbers and I thought, let's look at them – it's typical for a physicist to want to do that." His efforts to find a signal in that noisy data proved fruitful.

Later, when he and economist Professor Mike Spagat at Royal Holloway, University of London, analysed a database of 20,000 attacks in Columbia

and plotted the number of attacks against the number of people killed in each of them, they found that rather than seeing a classic bell curve – the graph that describes most things in nature, from height to lifespans of individual species – what they saw was a steeply sloped graph that quickly levelled off, with a long 'tail'. It reflected the fact that there had been a large number of attacks with a small number of casualties, and a small handful of attacks with a very high death toll. When they did the same with data that followed the 2003 invasion of Iraq, it showed exactly the same pattern.

What they'd discovered was a 'power law', a mathematical relationship found in phenomena right across science – everything from how the molecules in materials behave when they're heated, to the frequency of earthquakes and even the masses of stars (see 'What is a power law?', p78).

The power law's discovery in the realm of terrorism has a chilling consequence. But it also raises the question whether these seemingly random acts might actually be predictable in some way.

At the same time as Johnson was uncovering the power law relationship between the number of terror attacks and their scale, computer scientist ➤

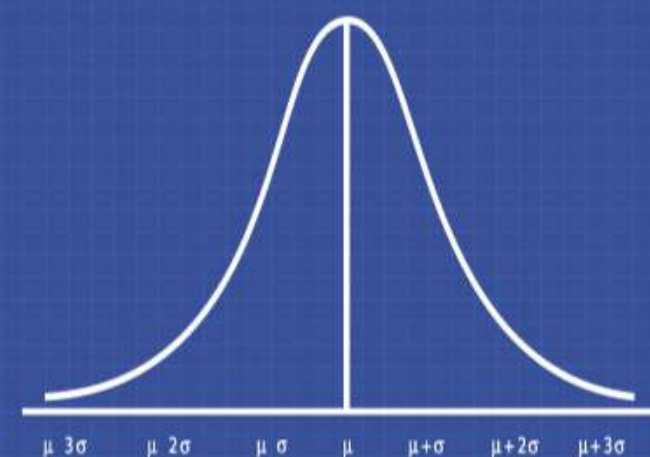
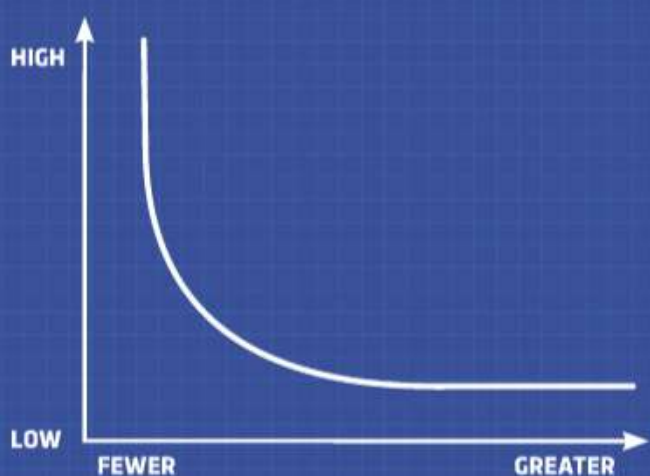
WHAT IS A POWER LAW?

It's a way to describe the relationship between two things, and states that a change in one thing results in a proportional change in the other thing. Take a square, for example: if you double the length of its sides, its area is increased four times, or by a power of two. Such relationships exist in all kinds of phenomena, from earthquakes to income levels.

Plot these power law relationships on a graph and it shows that the most common things are those at the smallest scale, whether that's the level of income or the size of earthquakes. But there are also a few extreme 'events', like massive earthquakes or huge incomes. That's not true of other things: plot people's height or weight on a graph and you'll get a bell curve (see bottom graph), in which most people are towards the middle and extreme 'events' are much less likely.

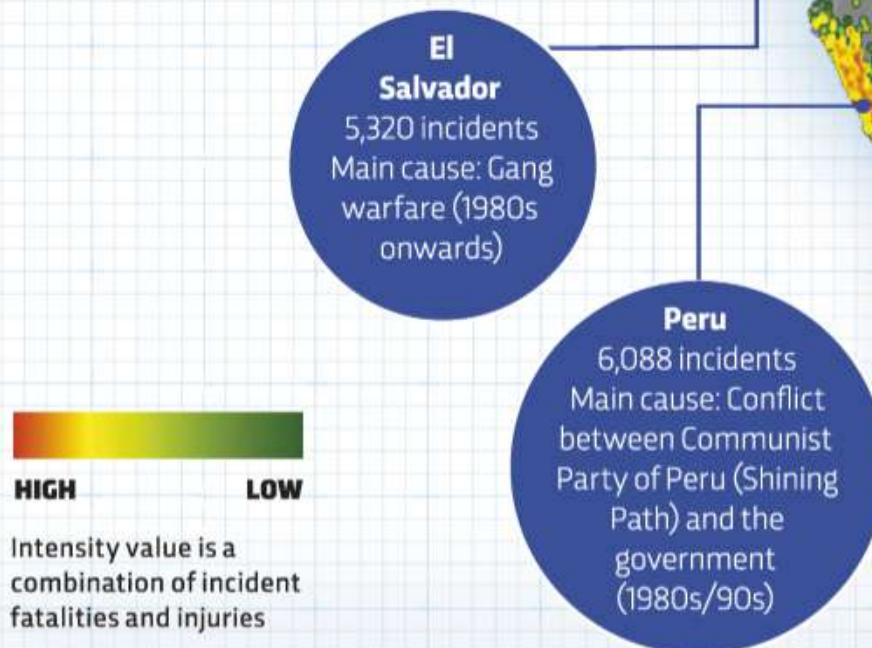
When it comes to terrorist events, a power law describes the relationship between the number of events and the number of people killed. It tells us that the 9/11 terror attack was not an anomaly – such an event is likely, statistically speaking, to occur again.

Written out, the power law is fairly simple: $Y = kX^{-a}$. Here X and Y are two variables that you're looking at the relationship between, say the number of terrorist incidents and the number of people killed. k is a constant, something that doesn't change over time and ' a ' is the law's 'exponent' – the 'power' bit of the equation that shows how much Y changes as X increases or decreases. With terrorist incidents, it was found to have a value of 2.5.



45 YEARS OF TERROR

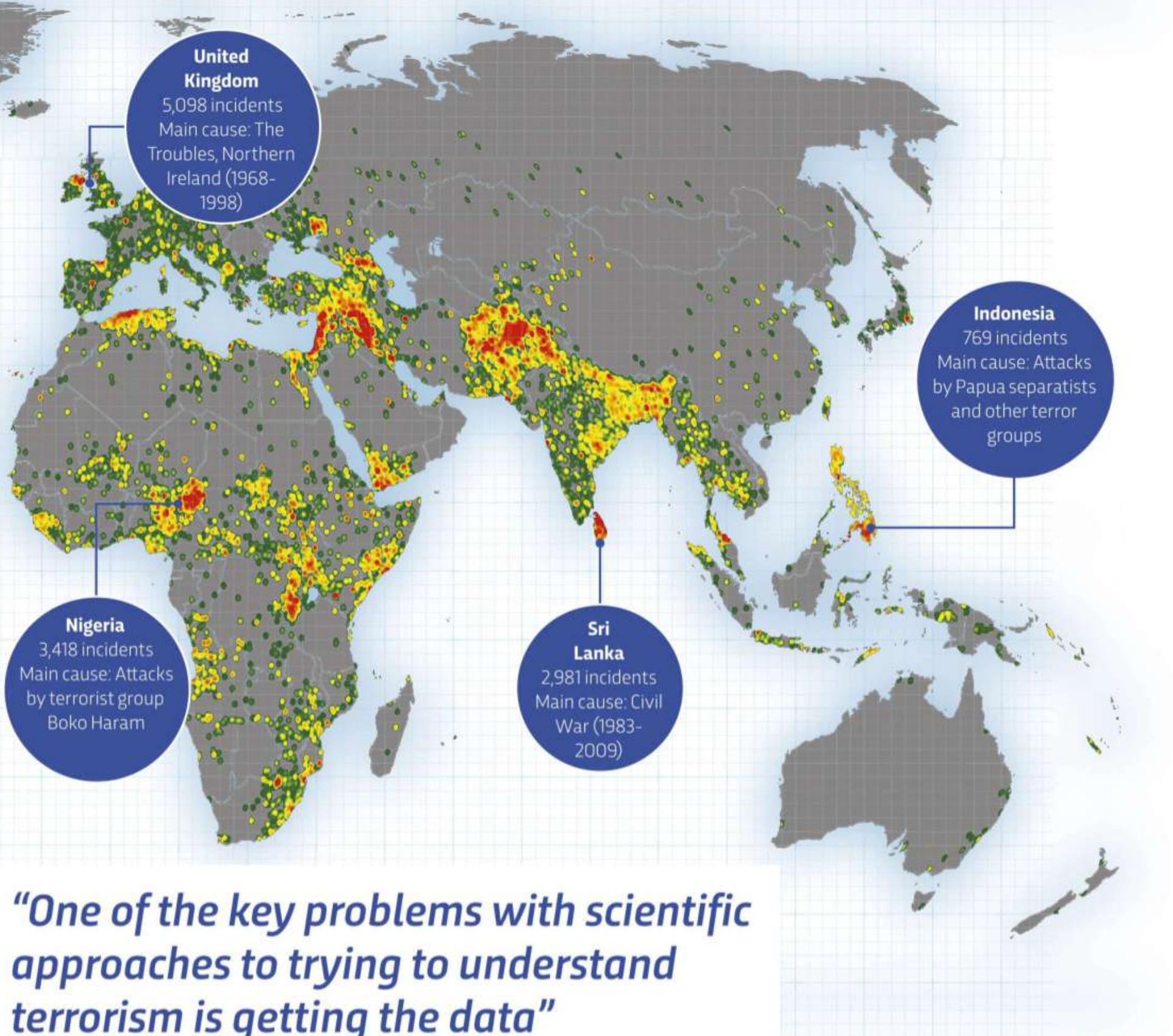
Heat map showing all known terror attacks between 1970 and 2015



Asst Prof Aaron Clauset at the University of Colorado at Boulder was doing just the same. Both of them were harnessing data from the Global Terrorism Database (GTD), a record of terror attacks around the world since 1970.

"One of the key problems with scientific approaches to trying to understand terrorism is getting the data," says Clauset. "For the most part, terrorists don't record their activities in nice structured formats. If you can't measure it, you can't do science with it."

The task of recording data on terror incidents has been taken up by staff and students at the University of Maryland, home of the National Consortium for the Study of Terrorism



and Responses to Terrorism (START). Here, computers use natural language processing to sift through 50 million newspaper articles per month and find reports of attacks. It's then down to a team of 10 analysts, helped by student volunteers, to read through the 16,000 articles the computers pick out per month and sift out any mistakenly identified as being terror-related. The articles weeded out are fed back to the computers so their artificial intelligence system can continually improve. The analysts then record 120 different variables about each attack such as the weapons used, the types of target and the number of people killed. The data they generate is released in chunks annually

and is freely available on the GTD website.

The data isn't perfect, because it relies on press reports. "There is inherently a bias," says Clauset. "If an event kills someone, it's much more likely to end up in the news media. If it's obviously terrorism, it's much more likely to be written about as terrorism. Small scale, non-lethal terrorism not claimed by any group is under-represented." But it's the best data there is, and when it's analysed it shows the power law in terror attacks, just like data from conflicts around the world.

The discovery of the power law relationship between the number of attacks and the number of people killed allows forecasts to be made. ➔



It's this kind of extrapolation that led to Clauset's forecast of the chance of another terrorist attack on the scale of 9/11 is 30 per cent over the next 10 years

"It allows us to extrapolate in a mathematically principled manner, to make statements about events that are incredibly rare."

It's this kind of extrapolation that led to Clauset's forecast that the chance of another terrorist attack on the scale of 9/11, that killed 2,996 people, is 30 per cent over the next 10 years. The maths can build expectations about the frequency of large-scale terror events, says Clauset. "But it doesn't allow us to predict when, why or how the next event will happen."

Some researchers, though, are using maths to try and predict who will be behind the next attack.

EXPLANATION REQUIRED

Before getting to the point of making predictions, there are other big questions to answer, such as why this 2.5 'power law of war' exists in the first place – especially given that the conflicts it describes are so different. "Some conflicts are Marxist, some fascist; it's not the terrain, because some are in the jungle, some in the desert, so it must be something else," says Johnson.

The first clue comes from the conflicts where the 2.5 power law doesn't hold, such as World War II or the Spanish or American civil wars,

where the conflicts were between two or more fairly evenly matched sides. In contrast, the conflicts where it does hold are asymmetric, involving two or more sides with very different resources at their disposal in terms of weapons and people.

"We thought about what we see when we heard about attacks in places like Iraq or Colombia. They sound like loose arrangements, where groups come together to do something and then vaporise," says Johnson.

When the number of these insurgent groups is compared the sizes of the groups, something familiar pops out – the 2.5 power law. In other words, the distribution of the sizes of the groups is almost identical to the distribution in the scale of attacks, with lots of small ones and a handful of very large ones. After all, it's logical that the handful of large groups it predicts will be able to carry out far more destructive attacks than the vast number of small groups or 'clusters' of fighters.



ABOVE LEFT: Inside a Special Operations Room run by London's Metropolitan Police

ABOVE: ISIS fighters on the border between Syria and Iraq in 2014

“By cluster, we don’t necessarily mean that the members have to walk round in a bunch, like kids in a playground,” says Johnson, “but that they are coordinated in some way, such as by some means of modern communication. So it can apply to a cluster of people in the desert during the Iraq era, but it also applies to more tech-savvy situations of a group of terrorists located in different places.”

This evidence for the number of groups and their size doesn’t come from groups identified on the ground. “It’s impossible to know the size of a cluster carrying out attacks,” says Johnson. But what is easier to get data on are the online groups of individuals who support a cause or ideology. In fact, the data is freely available, as most groups are visible online to encourage new recruits.

Johnson and his colleagues studied pro-ISIS groups that share operational information, such as advice on financing terror attacks or how to avoid drones. Where Facebook shuts extremist

groups down quickly, pro-ISIS groups seem to be more prevalent on other online platforms, which perhaps have fewer resources to check what’s being posted. In a study of open-access information on the platform VKontakte, based in Russia, Johnson found 196 pro-ISIS groups with over 100,000 followers. Although groups were shut down by moderators within weeks of being created, the members would just go on to form a new aggregate or join another existing one. It’s these groups that followed the power law in their scale. And this fluid online world of ISIS support, where groups coalesce, disappear and re-form, suggests a means to thwart these groups – split them up before they have time to form larger, more deadly groups.

IDENTIFYING POTENTIAL TERRORISTS

Having characterised this ecosystem of online groups, Johnson and his fellow researchers have now shifted their attention to how individuals move through them, finding groups that match their interests and shifting to new ones when groups are broken up. They found that despite there being many possible ways to move around, certain patterns emerge, and that individuals can be described in just a handful of ways. Some people, for example, will at some point express such extreme views that their account will be banned by moderators, while others will delete their own accounts, perhaps through fear of being linked to an extremist group.

To better understand how individuals move through these online ISIS-supporting groups, Johnson turned to a ‘stochastic walk model’, which predicts how people move through an imaginary 3D space. In this case, that space is the online ecosystem of pro-ISIS groups, and the destinations are getting banned, self-deleting or something else. Stochastic processes are those that randomly change over time and are found everywhere, from the fluctuations of electrical currents to the movements of gas molecules.

Not only is this allowing Johnson to develop timelines of movements of individuals through this online world, it’s also allowing him to study what determines an individual’s ultimate destination (in other words, banned ➔



or otherwise). “Part of it is the groups they pass through,” he says. “This is what we’re working on now. Is it worse if I go through two extreme groups without having a more spiritual group in-between, or is it worse if I go through a couple of spiritual groups and then on to an extreme one?”

It’s the people who end up being banned, the ones posting the most extreme content, who are of most interest to the authorities, says Johnson, because they are the most likely to carry out an attack. Fortunately, those who get banned most quickly tend to follow similar patterns in their movements, making them more predictable. And how this can be used doesn’t end with ISIS. Other forms of extremism exist online, such as far left and far right ideologies, and the findings about the movements of pro-ISIS individuals are likely to be more widely applicable.

The focus on groups and their influence is the right way to think about this, says psychologist Professor Alex Hasslam at The University of

Queensland in Australia. An expert on how groups influence individuals, he was involved in the BBC Prison Study in 2002 that saw volunteers spending time in a mock prison to see how they behaved.

“After a terror attack, it’s pretty standard for people to say, ‘He was a really decent person, I’m shocked at this,’” says Hasslam. “But it’s much more about understanding the groups they were in.”

Being able to predict who is more likely to engage in terrorism from their trajectory through online groups leads to an ethical question: what to do when someone who seems to pose a threat is identified? Johnson sees it simply as “an additional piece of information that the legal system can decide how to use,” but Clauset urges caution.

“The idea of looking at precursor signals or trajectories isn’t unreasonable,” he says, “but I think the standards for believing these things are correct must be very high, because we are talking about people’s lives here.” **F**

Sympathisers to far-right social patriot political party Espana 2000 perform the fascist salute

Andy Ridgway is a science writer based in Bristol.

THE ROBOCOPS ARE HERE

As robotic police head out on the street of Dubai, we look at the technology that's set to revolutionise law and order

WORDS: HAYLEY BENNETT



Dubai, it seems, is on a mission to dehumanise its police force. The city's streets will be patrolled by the OR-3 autonomous police car

1. ROBO ROZZERS

Visitors to Dubai's busy shopping arcades may be surprised to find themselves under the protection of a humanoid police robot. Though it has no mouth, the expressionless bot (see previous page) communicates in Arabic and English, and helps tourists navigate the city, as well as connecting them directly with police services via a touchscreen.

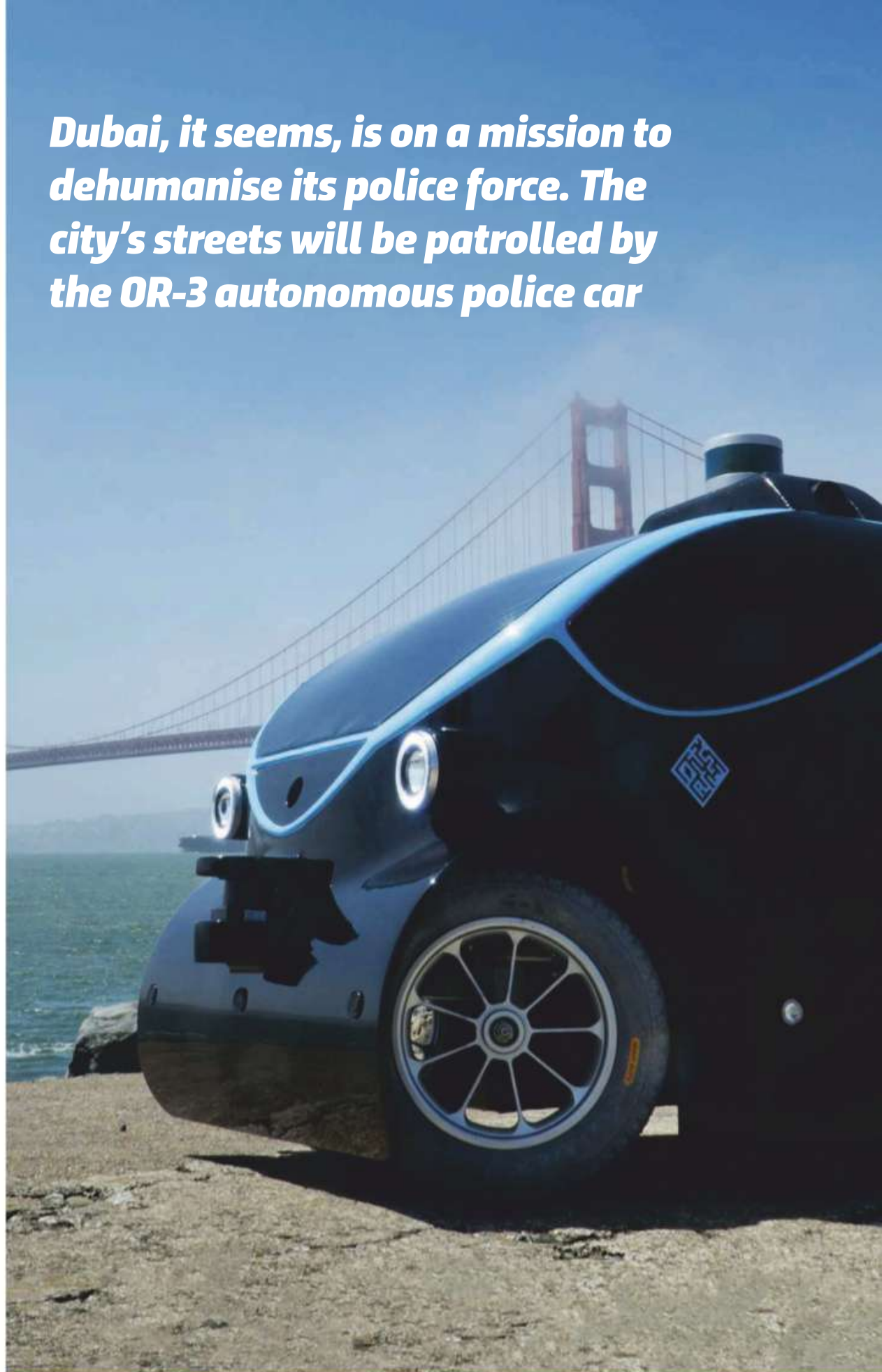
Dubai's answer to RoboCop dresses and salutes like a police officer but is actually from an existing family of robots known as REEM, built and programmed by the Barcelona-based company PAL Robotics.

"Citizens can use the robot to contact the Dubai police call centres, speaking through the integrated microphones, and accessing other police-related services such as paying traffic fines. The robot can also report any incidents to a command control centre," a source at PAL tells us.

REEM robots had already spent a number of years working at public events, so it was just a case of customising their software to include police functions, PAL says. The police version has face recognition software, meaning it could potentially catch a criminal by making comparisons with the police database. PAL hopes that the robots will become more accepted as people get used to seeing them around, and we might see them filling roles in healthcare and hospitality in the not-so-distant future.

PAL would not confirm whether it had any further robots on order for Dubai police, or if it would be upgrading the current model. However, Saif Salem Juma Ali Alkaabi at the Dubai police told us that "the numbers of robots will increase for sure". Its Smart Services department previously set a target of replacing a quarter of its on-patrol officers with robots by 2030. The Dubai government has also announced plans for a new model that makes the current officer look like little more than a glorified tourist information point. The 'RoboCop 2.0' will, apparently, be able to run at 80km/h (50mph), and be controlled by an on-board human pilot.

SHUTTERSTOCK



2. SELF-DRIVE SURVEILLANCE

Dubai, it seems, is on a mission to dehumanise its police force. The city's streets will be patrolled by the OR-3 autonomous police car, the Dubai police force announced in 2017. At under a metre high, the OR-3 is too small to accommodate a human passenger, but it doesn't need to. The vehicle boasts a range of high-tech navigation and data

collection tools: GPS, a laser scanner, thermal imaging and LIDAR – a remote-sensing method used in surveying. It's designed for 360° surveillance and can track down police suspects using its biometric scanners. Oh, yeah, and who needs police helicopters? The OR-3 comes complete with a mini-drone that can be launched for aerial surveillance.



3. SWAT-BOTS

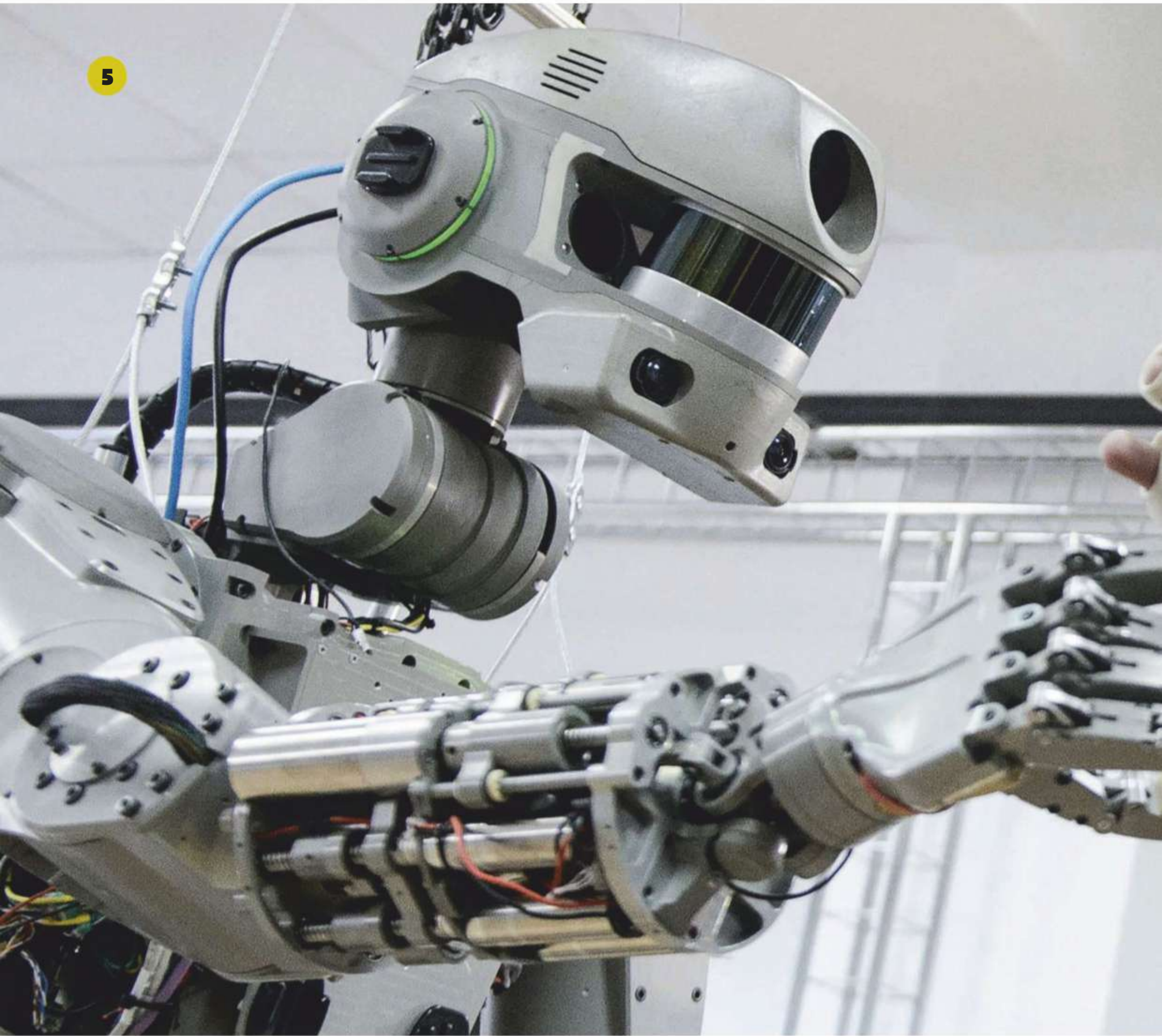
It looks like a tiny tank with a police shield attached, and that's basically what it is. The 'SWAT-Bot' is designed to batter down doors and protect tactical teams of up to 12 people when approaching armed suspects. It can also be operated remotely.

Created by twin brothers, Mike and Geoff Howe of Howe and Howe Technologies, it was developed in conjunction with Massachusetts police, although so far there have been no reports of the SWAT-Bot being used for anything but drills.

4. THE SECRET POLICE

Another tool for tactical teams, the Throwbot XT is a miniature stealth robot that weighs little more than a rugby ball and can be thrown – literally – into any situation where a human counterpart might attract too much attention. Once in situ, it can be directed to quietly survey its surroundings, transmitting video and audio to an operator. Its makers, Minneapolis-based ReconRobotics, claim that the Throwbot can see in complete darkness and can be used to locate hostages and armed suspects.

5



5. SHARP SHOOTER

Russian robot FEDOR is destined for the stars (okay, near-Earth orbit). The Russian space agency Roscosmos plans for the robot to pilot the unmanned *Federatsiya* spacecraft on its first mission in 2021. The bot's fine motor skills give it the dexterity to screw in light bulbs and drive cars, but have also led to speculation about other potential roles. That's because in April last year, FEDOR

was filmed being trained to shoot two guns at once, firing double-handed like a gunslinger from the Wild West, and both on target.

While Russian officials were quick to point out that they are not "creating a Terminator", some people have jumped to other conclusions. Meanwhile, scientists at Russia's Advanced Research Fund, which built FEDOR in



partnership with Android Technics, are also developing robots to assist special forces in the field. They are working on a prototype for a robot that will “deliver ammunition to the battlefield, support the sniper and, if necessary, help in evacuation of the wounded,” the organisation’s deputy head of robotics, Alexei Kononov, told the Russian news agency RIA Novosti in October 2017.

GETTY X2, KNIGHTSCOPE

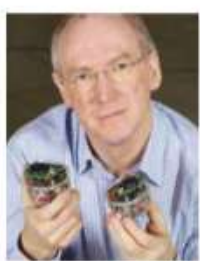
6. BOTS ON THE BEAT

A railway station in Henan province, China, has its own RoboCop in the form of the E-Patrol Robot Sheriff (below). Equipped with facial recognition software, it’s designed to identify and track criminals, and also functions as an environmental monitoring station thanks to its air quality and temperature sensors. These reportedly came in handy on the robot’s first day on the job, when it detected a fire.

Meanwhile, California has been trialling robotic security guards in shopping malls and car parks. The US-made Knightscope K5 (bottom image) works like CCTV, transmitting data to a control centre. Undeterred by a collision with a toddler and a ‘self-drowning’ incident in a fountain, Knightscope recently unveiled K5’s shiny new successor, K7 – a 3m-long buggy that can patrol on grass or sand.



ROBOCOPS: THE NEW FACE OF THE POLICE, OR AN ELABORATE PR STUNT?



Prof Alan Winfield, a robot ethicist at the University of the West of England, discusses the pros and cons of police robots

WHAT DO YOU THINK TODAY'S ROBOTS CAN USEFULLY CONTRIBUTE TO THE POLICE SERVICE?

The one positive thing that I can see is a kind of reassuring presence. That's if they're trusted. It depends on how people react to the robots, but robots moving around a shopping mall, for instance, could prove reassuring – even if not as much as real, live human police. Having said that, I do appreciate that there are cultural differences, and in some countries, particularly in the Far East, robots are likely regarded with a greater level of trust than in the UK.

THERE'S TALK OF ROBOTS BEING GIVEN GREATER POWERS. COULD THEY MAKE ARRESTS?

The power to arrest someone is a privileged duty because you are essentially making a judgment about whether that person has committed a crime. If a human makes that judgment and it turns out to have been incorrect, then they can be held accountable. But you can't sanction a robot: they can't be held responsible for their own behaviour, at least until the far-distant future.

SO ROBOTS COULD NEVER BE FULLY FLEDGED POLICE OFFICERS?

I'm not saying it's impossible that we could build robots that have some responsibility, but for something to be responsible in law, it's got

to have some kind of personhood. Giving a robot personhood right now is absurd – it's like giving your washing machine personhood, or your mobile phone. Think of a robot-like Data from *Star Trek*, a robot that effectively earns trust and genuine friendship from its human colleagues, that demonstrates its reliability over many years of companionship and actually cares about the people it works with. That's what we'd need in order to be able to assign it consequential responsibilities such as the power to arrest someone. I think we're looking hundreds of years into the future before we can build such a machine.

WHAT KINDS OF PROBLEMS COULD A ROBOT POLICE OFFICER ENCOUNTER?

There have been examples of robots being hassled by kids, although you can't really abuse a machine, as such. Another problem is the robot being 'gamed'. In other words, people will work out what its weaknesses are, where its senses are, and then try and back it into a corner or persuade it to go in a particular direction.

Another big worry that I have is hacking, and we know from experience that no systems are unhackable. We've seen incidents of driverless cars being hacked, and even devices apparently as benign as webcams. So a

"Another big worry I have is hacking, and we know from experience that no systems are unhackable"

malicious person could hack into a police robot and cause all kinds of havoc, particularly if they're remotely controlling the robot. All told, you've got a whole spectrum of potential problems with robot police, and these will all happen – there's no doubt about it.

WHO'S RESPONSIBLE IF SOMEONE IS INJURED BY A POLICE ROBOT, OR IF IT MAKES A MISTAKE?

The owner of the robot probably ultimately has responsibility, but if there was a manufacturing fault, it's no different to your car. If you crash into someone and cause injury, it's your responsibility, but if it turned out the crash was partly caused by a significant fault in the car, then the responsibility might be shared with the people who maintained your car – who fixed the brakes the last time, for example – or even with the car's manufacturers, who, for whatever reason, might have built in some design flaws.

DO WE NEED ANY NEW LAWS TO DEAL WITH POTENTIAL POLICE ROBOT INCIDENTS?

Robots are no different from any other manufactured object. They're human-made artefacts, and we have tonnes of legal history of accidents with machines, in which culpability is discoverable and people are held to account and end up paying for it, often through their insurance, of course. So I think it's quite wrong to give robots any special status in this regard. I suspect the new law that's needed is more around issues of transparency. So you've heard of a black box in an aeroplane – it's a flight data recorder, and when air accidents happen, the first thing that the investigators do is look for the recorder. It's absolutely crucial to finding out what went wrong in the accident. I think that robots, especially those in roles such as the police, absolutely must be fitted with a robot equivalent of the flight data recorder that basically records everything that happens to it. In fact, I wrote a paper on this: 'The Case For An Ethical Black Box'. I think it should be illegal to operate driverless cars, care robots or police robots without one.

THERE MUST BE SOME ADVANTAGES TO ROBOT POLICE OFFICERS. COULDN'T THEY BE COMPLETELY FAIR AND IMPARTIAL IN A WAY THAT A HUMAN CANNOT?

The experience of AI [artificial intelligence]



RoboCop, as depicted in the movies, is unlikely to be hitting the streets any time soon. Although his predecessors might...

has shown that this is not the case. It's very difficult to build unbiased AI systems. Face recognition algorithms are typically quite good at recognising white faces, but not other ethnicities, and this is simply a bias that reflects the fact that the datasets used to train the facial recognition algorithms have not been properly designed. So the idea that a robot would be more impartial is... I mean, it depends on the kinds of decisions it's making. Unfortunately, there are examples of bias in AI systems being reported all the time.

SO ARE POLICE ROBOTS MORE OF A PUBLICITY STUNT THAN A REALISTIC APPLICATION FOR HUMANOID ROBOTS RIGHT NOW?

Yes, I think the worry is that it can be a PR stunt, particularly if you're a country that is very serious about investing heavily in robotics and AI. I think it helps to raise the visibility and the profile of that level of investment so, yes, there's probably a big publicity aspect to it. 📢

Hayley Bennett is a science writer based in Bristol.



Watch *Law and Order: Dubai*, which looks at the city's new police bots [bbc.in/2APP5CV](https://www.bbc.com/news/technology-55555555)

FIGHTING CRIME

THE FUTURE OF



GUNSHOT
TRIANGULATION
IN PROGRESS...

FIGHTING CRIME

DRONES SENT
TO INVESTIGATE

Criminal masterminds had better watch out. Scientists are on their tail and have some clever new ways to catch them. Discover the advances that are revolutionising criminology and forensics

WORDS: ANDY RIDGWAY ILLUSTRATIONS: VLADO KRIZAN



PREDICTIVE POLICING

CAN WE PREDICT CRIMES BEFORE THEY HAPPEN?

It's 4:30am on a Friday morning in August and there's a heavy police presence in a quiet London suburb. It's a respectable, leafy area and right now, nothing is happening. In fact, it's been quiet for the past few days. But the officers are on high alert. They've been sent at the say-so of a computer that's calculated, on the basis of the data fed into it, that a wave of break-ins is highly likely within the next 24 hours. In other words, they're policing crimes that they think will happen, rather than ones that have happened. This is predictive policing. And it's about to get more sophisticated.

The idea of predicting where crimes will take place isn't new. For decades now, police forces in the UK and US have been creating 'hotspot' maps that identify the areas where most incidents are taking place, and then sending more police officers to those areas. Predictive policing takes this to the next level, crunching big data using algorithms based on those that help to predict

when and where the next earthquake aftershock will be, or how a disease will spread.

These algorithms generate information that police officers can act on, and it seems to work. In tests, their predictive powers appear to outperform the more traditional techniques used by crime analysts. Their successes have led to predictive policing being adopted by Kent Police.

But not everyone's convinced about predictive policing – or how it's implemented at least. Among them is criminologist Prof John Eck at the University of Cincinnati. His problem isn't so much with the predictive policing software itself, but the idea of sending out large numbers of staff to patrol problems highlighted by the algorithms. "Why would you want to keep sending large amounts of expensive public servants to these locations?" he says. "Instead, we should be asking why this location has a persistent crime problem, and what we can

do to keep it from happening." Eck would prefer it if the police encouraged owners of businesses and other properties highlighted as crime hotspots to step in and make changes, such as shops with high shoplifting rates repositioning displays. Critics have raised other concerns too, such as the possibility of crimes simply shifting to other locations when problem areas are targeted by the police.

But predictive policing is becoming more widespread, and it could be about to change radically. In 2017, a bunch of mathematicians led by Prof Mark Girolami at Imperial College London were awarded £3m from the government to take predictive policing to the next level. Whereas today's tools just rely on crime data – such as the locations, dates and times of incidents – Girolami and his team are working on how to integrate the likes of Twitter feeds, newspaper reports and socioeconomic data to sharpen the predictions. Text documents will be converted, or 'coded', into numerical representations, with counts of words and phrases – such as descriptions of assaults or break-ins – to highlight geographical areas of concern. "All of these streams of information will be coded and integrated using our 'secret sauce'," says Girolami, referring to the complex maths that will draw all of this disparate data together. And this new predictive tool aims to work out the extent to which crime will be displaced to a neighbouring area when police numbers in the original area suddenly shoot up. "Our models will be able to propagate what would happen," says Girolami.



University of California researchers demonstrate predictive policing with Los Angeles police

HEAD CAM
OFFICER BO
HOLD AR: AD

SHUTTERSTOCK ILLUSTRATION: VLADO KRIZAN

AUGMENTED CRIME SCENES

Being the first police officer to arrive at a crime scene is a stressful business. Are the culprits still here? Is it safe for me to walk around? Does anyone need medical help? In these circumstances, it's easy for what might later turn out to be a vital piece of evidence to be 'polluted' in some way – trodden on, knocked over or mishandled. But soon, officers arriving at such scenes may have the finest minds in crime scene investigation to guide their every move, even if they're working at the other end of the city.

The idea is to use augmented reality, where a view of the real world is 'augmented' in some way with digital data. Researchers at Delft University of Technology in the Netherlands have been working with Dutch police, the Netherlands Forensic Institute and the Dutch Fire Brigade to develop a system in which crime scenes get overlaid with information from a CSI expert so early arrivers know what to bag up as evidence or investigate further.

In one trial of the technology, officers were faced with a mock ecstasy lab in the kitchen of an apartment. A smartphone mounted on an officer's shoulder beamed live video to a crime scene investigator who then annotated what they could see, highlighting the chemicals and equipment that would need to be removed for analysis. The officers on the ground viewed the scene and annotations through a second smartphone they were holding and, in another test, the smartphones were replaced with augmented reality headsets.

SCENES GET OVERLAID WITH INFORMATION FROM A CSI EXPERT SO EARLY ARRIVERS KNOW WHAT TO BAG UP AS EVIDENCE

EXTRAORDINARY EVIDENCE

Even the tiniest scraps of evidence can help to catch a criminal

GUNSHOT FORENSICS

Gunshots ring around a city centre street. One man lies dead in the road and another tells the police he fired his gun in self-defence after being shot at. No one saw what happened. The one thing the police do have is video footage from a mobile phone, while it doesn't actually show the shooting, the sounds of the gunshots have been captured. Dr Robert Maher at Montana State University is the man to call. By firing assorted weaponry near a semicircle of 12 microphones, he has developed a database of soundwaves produced by different guns. The aim is to enable different gun types to be distinguished from a sound recording, helping police unpick exactly what went on in cases like our shoot-out.



MICROBIAL FINGERPRINTING

It's a slightly unsettling thought that each of us sheds around 30 million bacterial cells from our bodies every hour. They waft into the air and cling to objects we've touched, like furniture and mobile phones. The community of microbes that live on and in our bodies, our microbiome, is also unique. Soon, criminals may be linked to a crime scene by the trail of bacteria they haplessly leave behind. In one study, Dr James Meadow, then at the University of Oregon, found that people could be identified simply from the invisible cloud of bacteria they left in the air – even when the air was sampled four hours after they had left the room.



WHAT'S IN A HAIR?

Give a strand of your hair to Dr Glen Jackson at West Virginia University and he can tell your age, sex, what you eat and how much you exercise. For police with little to go on from a crime scene other than a few bits of hair, this information can be like gold dust. Jackson and his team measure the ratio of isotopes – atoms of the same element with different numbers of neutrons – within the 21 amino acids found in keratin, the main component of hair. So far, they have found 15 isotope ratios that provide a window into who someone is.



SCENT OF A VILLAIN

In the future, vanishingly small traces of perfume or aftershave on a shirt could be enough to bring an attacker to justice. Fragrances are notoriously difficult to detect because they are made up of volatile molecules that evaporate rapidly. But a team led by PhD student Simona Ghergel at University College London has found that the cocktail of compounds that make up perfumes can be transferred between clothes and subsequently detected. The highly-sensitive detection technique is known as 'gas chromatography-mass spectrometry'. In one test, when two fabrics had been in contact for just one minute, 15 out of 44 fragrance components in a male cologne were found.

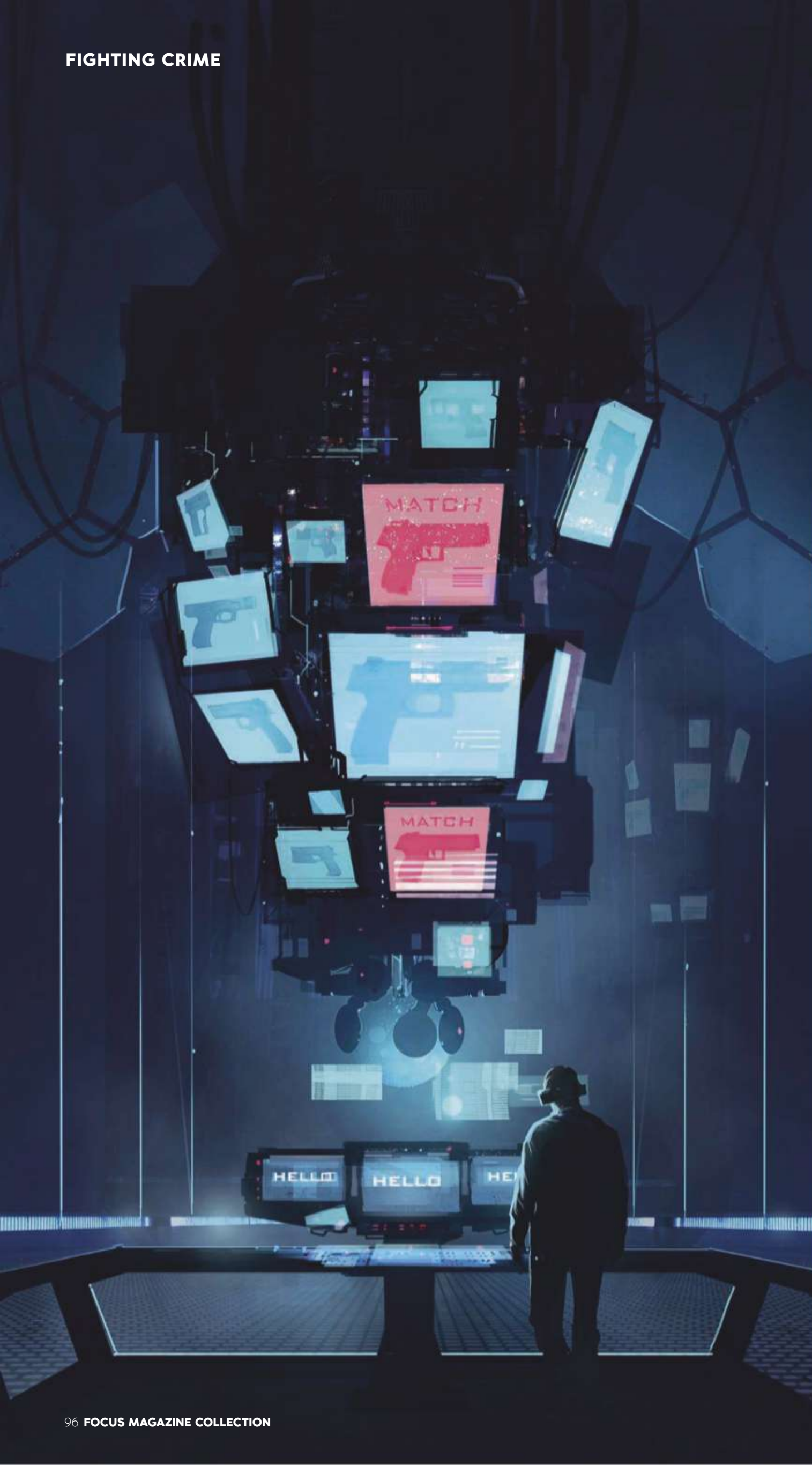
E.COLI
GENOME IDENTIFIED
SUSPECT ORWIN ALBANI

ARMED ROBBERY
AGGRAVATED ASSAULT

VIEW FULL PROFILE: Y/N




POLICE LINE **POLICE LINE** **POLICE LINE** **POLICE LINE**



AI DETECTIVES

There has been a spate of armed robberies in the city. And detective VALCRI has been tasked with scanning thousands of records of previous crimes to find patterns and connections that could help track down who is responsible. The thing is, VALCRI isn't human.

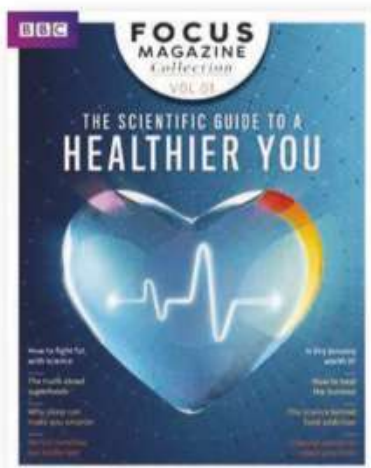
VALCRI, or Visual Analytics for Sense-making in Criminal Intelligence Analysis, is an AI system that can scan police crime reports, interviews, videos and pictures, interpreting words and recognising faces. Its aim is to identify links between crimes that might provide detectives with an all-important breakthrough. These links may be similarities in the modus operandi of the thief, a reoccurring weapon, or similar descriptions by witnesses. Funded by the EU and led by Prof William Wong at Middlesex University London, VALCRI can learn, too. When a crime analyst decides whether a piece of evidence identified by the system is relevant or not, it will use that information to improve future searches.

VALCRI isn't alone – other AI systems for crime detection have been developed to do everything from sifting large volumes of documents for clues in fraud cases to helping forensic teams determine how many people have contributed to a large, multi-person DNA sample – something that's tricky to fathom at present. 

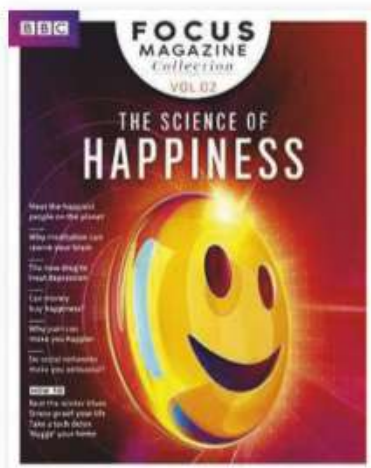
Andy Ridgway is a science writer based in Bristol.

FROM THE MAKERS OF
BBC FOCUS MAGAZINE

**ONLY
 £9.99**
 EACH INCLUDING
 P&P*



Get fit and healthy!
 Discover the science
 behind what really
 makes you healthier and
 fitter, as experts reveal
 how to eat, exercise
 and sleep well.



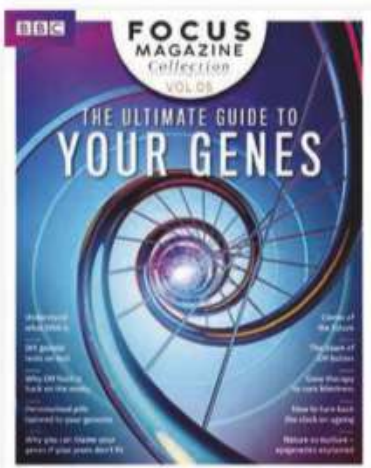
Discover the science
 behind how to be happy,
 from stress-busting tricks
 to taking a tech detox.
 And find out why the
 happiest people on the
 planet keep smiling.



From the depths of the
 ocean to outer space,
 this special issue joins
 the expeditions that are
 pushing the boundaries
 on our quest to reach the
 final frontiers.



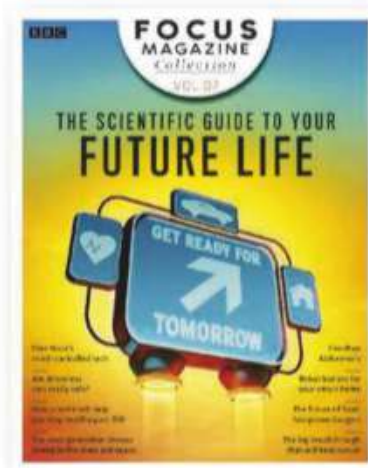
Find out how we can fix
 climate change, beat mass
 extinction and protect
 the planet. Experts reveal
 solutions to overfishing,
 plastic waste, flooding
 and air pollution.



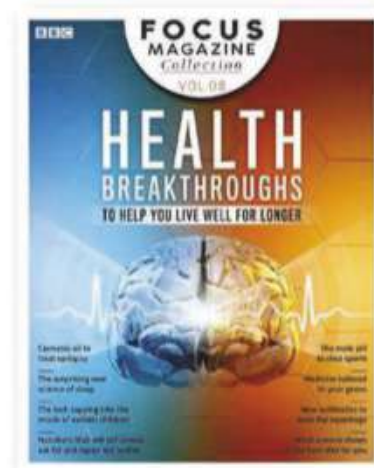
Each life form on this
 planet has a unique
 genetic code – DNA. Now
 geneticists are using DNA
 to improve our health,
 eliminate hunger and
 even bring back animals...



Quantum physics,
 space-time, black holes,
 multiverses... The nature
 of the Universe can make
 your head spin. But this
 special edition can help
 make things easier.



From smartphones to
 smart homes, technology
 and science are
 revolutionising our lives.
 Discover the innovations
 that will change your
 world in years to come.



Discover how this
 exciting new era of
 breakthroughs in
 medicine will increase
 our lifespans, revitalise
 healthcare and even
 slash recovery times...

Order online: **www.buysubscriptions.com/focuscollection**
 or call us on **03330 162 138[†]** and quote **FOCSPEC**

[†]Calls from landlines will cost up to 9p per minute. Call charges from mobile phones will cost between 3p and 55p per minute but are included in free call packages. Lines are open 8.00am - 6.00pm weekdays and 9.00am - 1pm Saturday for orders only. *Subscribers to BBC Focus Magazine receive FREE UK POSTAGE on these special editions. Prices including postage are: £11.49 for UK residents, £12.99 for Europe and £13.49 for Rest of World. All orders subject to availability. Please allow up to 21 days for delivery.

MY LIFE SCIENTIFIC

KERRY DAYNES

Forensic psychologist Kerry Daynes on psychopaths, stalkers and the surreal side of working with serial killers

WORDS: HELEN PILCHER

WHAT DO YOU DO?

I've spent a lot of my career working with people who have severe personality disorders, including psychopaths and sexual offenders. It was my job to make them less of a risk.

WHAT'S IT LIKE WORKING WITH THEM?

It can be surreal. I worked with one serial killer, a trained butcher, who dismembered people. You have to build up a rapport with people in order to work meaningfully with them, so we cooked together. He taught me how to bone a turkey! All along I was aware these were the same skills that he used on his victims.

WHICH ARE YOU MORE LIKE, CLARICE STARLING OR CRACKER?

Neither, these fictional characters are 'profilers'. Cracker was an emotionally damaged Scot who tramped all over crime scenes. It's an inaccurate portrayal of what people like me do. But anything that sparks the public's interest in science and psychology is okay in my book.

WHAT WAS IT LIKE THE FIRST TIME YOU MET ONE OF THESE OFFENDERS?

It was a baptism of fire. I was 21 years old, doing research in a high-security prison, interviewing men who had raped and murdered their victims. While it was daunting, I was able to separate myself from it emotionally and get on with the job. In the end, the

prison officers were more difficult than the offenders.

HOW DO YOU MEAN?

It was an incestuous, institutional male environment. The guards ordered me to remove my shoes because they were 'too sexy'. They even ran a book on who would be the first to sleep with me! Things have moved on since then and I don't work in prisons any more. Forensic psychology is actually a very female world.

DOES YOUR PROFESSIONAL LIFE EVER SPILL INTO YOUR PRIVATE LIFE?

I became the victim of a stalker. He watched me, bought websites in my name and said damaging things about me in public. The police could only issue a harassment warning, but I took civil action against him. It stunned me how inadequate the current laws are, but it did give me first-hand knowledge of what it's like to be a victim.

DO YOU EVER THINK ABOUT QUITTING?

I've worked with the most misogynistic, dangerous men imaginable. It takes its toll. I made a conscious decision a while



ago to start working more in general mental health and with victims. I've also branched into the corporate sector.

DO YOU MEET MANY PSYCHOPATHS IN THE BUSINESS WORLD?

Yes! One in every 100 people are psychopaths and 20 per cent of CEOs score highly on psychopathic traits. Moderate levels of psychopathic-like traits can be useful, as long as they're tempered with compassion and humility. I draw on my unique experiences to teach skills to business leaders.

I THINK I AM GOING TO WORRY ABOUT YOU. PROMISE ME YOU'LL BE OKAY?!

I'm pretty resilient. I come from a very stable and 'normal' background; that helps. I also have two enormous dogs, Humphrey and Fozzchops. When the complexity and inhumanity of some humans feels a little overwhelming, the simplicity and innocence of a happy dog is a great antidote. 🐕

"I worked with one serial killer, a trained butcher, who dismembered people"

GALAXY

ON GLASS

*a **big** impact in any room*




Spectacular wall art from astro photographer Chris Baker.

See the exciting new pricing and images!

Available as frameless acrylic or framed and backlit up to 1.2 metres wide. All limited editions.

www.galaxyonglass.com | chris@galaxyonglass.com

Or call Chris now on **07814 181647**

The background features a dark blue to black gradient with a fine grid pattern. Overlaid on this are several concentric circles. The innermost circle is a vibrant red, while the outer rings transition through shades of purple and blue. The text is centered in the upper half of the image.

Discover how forensic scientists really
investigate a crime scene, get CIA
secrets on how to extract the truth, go
inside the minds of psychopaths and
serial killers, and find out how cops will
fight the bad guys in the future.

FROM THE MAKERS OF **BBC FOCUS** MAGAZINE